PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 1/32 — A1

(11) International Publication Number: **WO 00/22811**

(43) International Publication Date: 20 April 2000 (20.04.00)

(21) International Application Number: PCT/JP99/05629

(22) International Filing Date: 13 October 1999 (13.10.99)

(30) Priority Data:

09/173,086	14 October 1998 (14.10.98)	US
09/276,841	26 March 1999 (26.03.99)	US
09/365,002	2 August 1999 (02.08.99)	US

(71) Applicant *(for all designated States except US)*: CANON SALES CO., INC. [JP/JP]; 11–28, Mita 3–chome, Minato–ku, Tokyo 108–0073 (JP).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: NUNALLY, Patrick, O'Neal [US/US]; 970 West Valley Parkway, Escondido, CA 92029 (US).

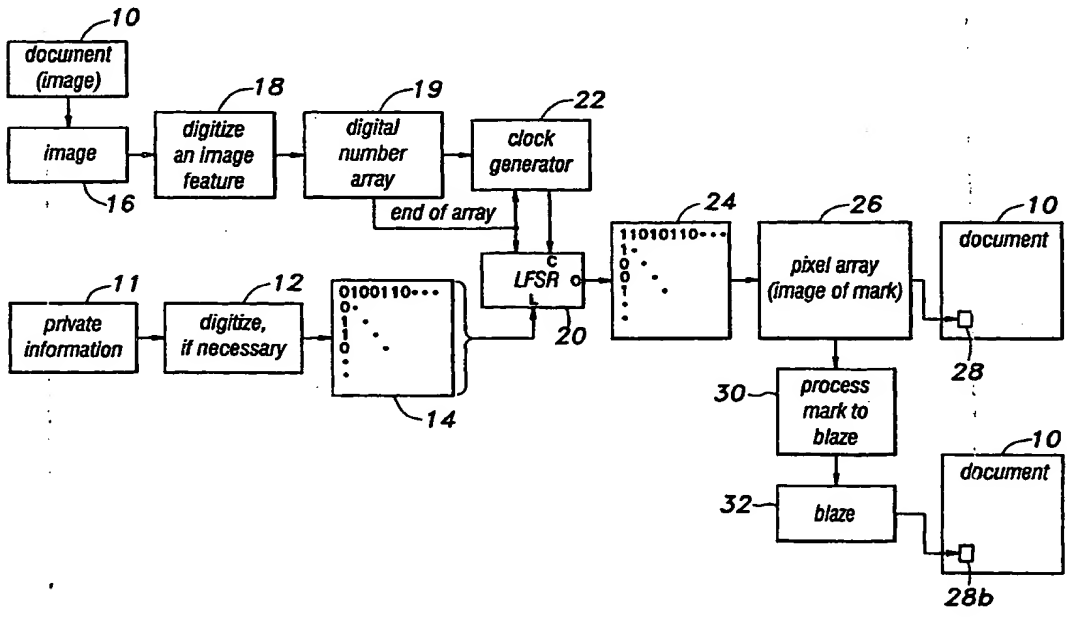
(74) Agent: OSHIMA, Yoichi; Kitagawa Building, 7th floor, 6–42 Kagurazaka, Shinjuku–ku, Tokyo 162–0825 (JP).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(54) Title: DOCUMENT AUTHENTICATION USING A MARK THAT IS SEPARATE FROM DOCUMENT INFORMATION



(57) Abstract

A digital mark is derived or created for placement on a document or image to identify, authenticate, or verify the origins of the document or image. Private information is received and digitized. The digitized private information is scrambled in response to the contents of the document or the image. The scrambled private information is formed into a mark. The mark is placed on or in the document or image, apart from the information of the document or image.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

DESCRIPTION

DOCUMENT AUTHENTICATION USING A MARK THAT IS SEPARATE FROM DOCUMENT INFORMATION

TECHNICAL FIELD

This invention concerns the use of marks to identify and/or authenticate documents, images and texts. More particularly, the invention concerns the identification and/or authentication of a document, image or text by means of a mark on the document, image or text that is separate from information that the document, image or text contains.

BACKGROUND OF THE INVENTION

A document contains information. According to an authoritative definition, a document is"... information and the medium on which it is recorded... ". In this regard, a document can be embodied in an image on a piece of paper, written information on a print-supporting medium, and electronic or optical data on a storage medium. Examples of common documents abound. Checks, photographs, movies on film or video, audiotapes, CD's, and passports are examples of documents. The present invention is applicable not only to documents but also to images and texts. In this regard, it is also possible to regard images and texts as variations of documents which are equally covered by the present application.

An image is a perceptible representation of something. An image may be evident to the eye. An image may also be perceived by a machine. In this latter regard, the IBM Dictionary of Computing, 10th Ed. (August 1993) defines an image as: "An electronic representation of a picture produced by means of sensing light, sound, electron radiation, or other emanations coming from the picture or reflected by the picture. An image can also be generated directly by software without reference to an existing picture ..." (p. 325). In the same entry, a second definition of an image is "an electronic representation of an original

document recorded by a scanning device." When used herein, the term "image" refers both to a visually perceptible object and also to an electronic representation of such an object.

In the Oxford Dictionary of Computing, Fourth Edition, 1996, a "document" is defined at page 149 as a "piece of text considered to be a single item and usually stored as a file. The document might be a letter, a report, a chapter, etc ....". In the IBM Dictionary of Computing, Eighth Edition, 1987, one definition of "text" is as follows: "A graphic representation of information on a output medium. Text can consist of alphanumeric characters and symbols arranged in paragraphs, tables, columns, or other shapes." ibid, p. 435.

It is increasingly important to be able to identify, authenticate and/or validate documents. In the past, such functions have been provided, for example, by the "chop" on a sheet of calligraphy, the account number on a check, a photograph on a passport, and a signature or thumbprint on a testament. The purpose of such measures is to prevent the illegal, unauthorized, unscrupulous, or nefarious use of original documents and their authorized copies. Consider, for example, the unauthorized use of a counter check that identifies a checking account depositor correctly. Without a discernable account number, the check will not be authorized for payment. However, the depositor will be assured of clearance of a check that bears both her account number and signature.

In the modern world of digital information; the ease with which documents can be obtained, copied, modified and transferred necessitates the provision of corresponding means for document identification, authentication and/or validation.

In this application, the term "digital mark" (or, simply "mark") is used to signify the existence of a digital object that may be appended, added to or placed on a document for the purposes of identifying, authenticating, or otherwise validating the document. The digital object embodying the digital mark is typically derived from signals representing information beyond that which is

apparent in the document. In this regard the term "digital object" signifies a perceptible or discernable object that is, or is created or derived from a digital representation that may be a vector, array, or sequence of ones and zeroes, or of pixels. Once created or derived, the mark may be appended to the information in the document, separately from the information, or may be embedded in the information so as to make it difficult to perceive when the document's information is comprehended in a content-appropriate manner. Thus, for example, an audiotape may have a digital mark woven into the audio information in such a way as to be imperceptible to a listener, but tractable to authenticating means that knows how and where to find the mark.

Digital marks that are perceptible and separate from the information in the document which they identify, authenticate and/or validate have the advantage of being relatively simple and inexpensive to locate and to process. No special means are necessary to perceive and extract the mark from the information contained in a document. Decoding the mark is simply a matter of applying a process that is inverse to that utilized for generating the mark. Any document without the mark will be presumed to be unidentifiable, inauthentic, or otherwise invalid.

BRIEF SUMMARY OF THE INVENTION

The invention provides derivation of a digital mark that is to be placed in a document apart from the information that the document contains. The invention is based on the critical realization that a robust mark may be derived by a process that combines the information in the document with private, extra-documentary information. The process receives the private information as an input and then scrambles the private information in response to the information in the document.

Scrambling is a process of pseudo-randomization of the input private information that may be accomplished, for example, by means of a linear feedback shift register (LFSR) clocked in response to the document information. The scrambled private information provides a digital mark that may be placed in

or on the document, apart from the information content of the document. In a particularly useful embodiment, the digital mark is processed to create a "blaze" by image processing that is analogous to "smearing" the pixels of an image.

In this regard, the scrambling is particularly efficiently accomplished by seeding an LFSR with the private information and then clocking the operation of the LFSR in response to the document information.

The invention also provides use of a digital mark to apprehend or enter information in the contents of an image such that the information uniquely identifies the image and copies of the image. Such identification can be used, for example, to identify an image or to authorize its copying by electronic means.

This aspect of the present invention is based on the critical realization that a uniquely generated mark can be correlated with the contents of an image to either apprehend information in or to enter information into the contents of the image. In either case, the information yields a unique signature identifying the image and any copies made of it.

The process utilizes a mark created by scrambling private information in response to information in the image. The mark, itself in the form of an image, is then correlated systematically against a succession of portions of the image. In one embodiment, the information is extracted from the results of the correlation. The information is used to derive a signature. In another embodiment, the mark is systematically correlated with a succession of image portions and one or more image portions are altered by algebraic addition of the image of the mark in such a manner as to insert or change information in the image. In this case the information inserted into or changed in the image imprints a signature that uniquely identifies the image.

In either embodiment, the image can be identified, using the mark to once again derive the signature. In either embodiment, copies of the image can be identified and/or authenticated by correlation of the mark with the image portions and comparison of the information derived therefrom with the previously-derived

signature of the image.

The invention also provides use of information hidden in the text of a document such that the information uniquely identifies the document. Such identification can be used, for example, to identify a document or to authorize its copying by electronic means.

This aspect of the present invention is based on the critical realization that a unique index can be generated in response to an image of the document. The index establishes a basis for coding information into text in the document that is hidden from sight. The process utilizes an index generated by scrambling private information in response to the image of the document. The index points to a page in a code book that contains "text kernels" - fragments or elements that are combined with other text kernels to yield text characters such as characters, letters, numerals, punctuation marks, and so On.

The indexed kernel is compared against the characters in the text of the document to identify characters that contain the kernel. Those characters are altered slightly in a manner that encodes information into the text. The alteration is imperceptible to human sight, but can be detected by machine' in order to decode the information and, using the decoded information, identify the text. Thus, originals and copies of the document can be identified, using the information hidden in the text contained in the copies.

Accordingly, a primary object of this invention to cause the generation of a digital mark by scrambling private information in response to the information of a document that is to be marked.

A second object of the present invention is to identify an image based upon information in the image that is obtained by comparing a unique mark with the contents of the image.

A third object of the present invention is to make such a comparison by systematically correlating the image content of the mark with the image content of a succession of portions of the image.

A fourth object of the present invention is to hide information in the text of a document in such a manner as to make the information imperceptible.

BRIEF DESCRIPTION OF THE DRAWINGS

These objectives and other advantages become evident in when following detailed description is read with reference to the below-described drawings, in which:

Fig. 1 is a block diagram organized to illustrate the functional components and operational flow of a system and a process that create a digital mark according to the invention;

Fig. 2 illustrates a document embodied in an image;

Fig. 3 is a grey scale image of the spectral energy in the tiles of the image of Fig. 2;

Fig. 4 is a computer memory diagram illustrating an array of digital numbers representing the spectral image of Fig. 3;

Fig. 5 is a block diagram illustrating the operation of a clocked linear feedback shift register employed by the invention to obtain a digital mark from input private information according to the invention;

Fig. 6 illustrates the incorporation of encryption into private information processing;

Fig. 7 is a block diagram illustrating how a blaze is derived from a digital mark according to the invention;

Fig. 8 illustrates a representative industrial application of this invention;

Fig. 9 illustrates how a blaze generated according to the invention is used to identify, authenticate, or otherwise validate an image;

Fig. 10 illustrates upon image with a blaze generated according to the invention is validated in response to input private information;

Fig. 11 is a flow diagram illustrating a computer-executed method according to the invention;

Fig. 12 is an illustration showing tiling of the image of Fig. 2;

Fig. 13 is a block diagram illustrating how tiles of the image of Fig. 2 are correlated with a mark's image to create a correlation map;

Fig. 14 is a block diagram illustrating how information extracted from the correlation map is used to derive a unique signature identifying the image of Fig. 2;

Fig. 15 is a block diagram illustrating how information is inserted or changed in the image by correlating the mark's image with the content of the image;

Fig. 16 is a flow diagram illustrating a computer-executed method according to the invention;

Fig. 17 illustrates a representative industrial application of this invention;

Fig. 18 illustrates how a signature is used to identify, authenticate, or otherwise validate an image;

Fig. 19 illustrates how a copy of an image with an inserted signature is identified, authenticated, or otherwise validated;

Fig. 20 is a block diagram of a system according to the invention for hiding information in the text of a document;

Fig. 21 is an illustration of data structures used by a coder that hides information in text according to the invention;

Fig. 22 is a schematic illustration of a document containing text and illustrating how information is hidden therein;

Fig. 23 is a schematic representation of a pixilated image of a text character T, showing how the image may be adjusted to encode information that is hidden in a document containing the character; and

Fig. 24 is a flow diagram illustrating a process according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

My invention concerns a method and an apparatus for generating a mark to be placed on a document, apart from the document's contents, that identifies,

authenticates, or otherwise validates the document. Relatedly, a document is defined in the IBM Dictionary of Computing, Eighth Edition (March 1987), as "information and the medium on which it is recorded that generally have permanence and can be read by humans or by a machine... ". A document may be a photograph, a graphic printed by a computer system, text, a book, a digitized image in storage, and so on. Generally, no matter what the instrument of perception (human or machine) I consider a document to contain information that may be subjected to a lossy type of compression and still be perceptible when decompressed.

Fig. 1 is a block diagram organized to illustrate the functional components and operational flow of a system and a process that creates a digital mark according to my invention. The digital mark is derived, created, or otherwise generated in order to be placed in or on a document 10 for the purpose of identifying, authenticating, or otherwise validating the document 10. The mark is derived by processing private information 11 in response to the contents of the document 10. In this regard, the private information may comprise any type of information in any form that can be transformed into a digital representation and that is private to a person, organization, or machine having some relationship to the contents of the document 10. The private information 11 may comprise, for example, a private number set or sequence such as a social security number, a driver's license number, a DNA sequence, or a telephone number. Private information may also comprise a private character set or sequence, a private alphanumeric set or sequence, a private graphic, a private image, a private document, or a private code (a genetic code, for example). It is necessary that the private information 11 be repeatable in the sense that, from one operation of the system and process of Fig. 1 to another, the private information will not change. In this regard, a signature would be inappropriate, given the variability from one instantiation to another. However, an image of the signature might serve satisfactorily as the private information 11. The private information 11 is input to

a digitizing process 12 which reduces the private information to a digital electronic form having a predetermined size. For example, assume that the private information 11 consists of a special security number input in standard decimal form. Assume that the output of the digitization element or function is constrained to be a digital sequence of 8K bits. In this case, the digitization element or function 12 would convert the social security number into digital form and replicate the digital form as many times as is necessary to provide a sequence of 8,000 bits. The digital form of the private information is represented by a two-dimensional array 14 of ones and zeroes ("binary digits" or "bits") that would reside, for example, in the memory of a computer. The two-dimensional array 14, may of course be assembled into a 1 x 8,000 bit vector by conventionally scanning it row by row from top left to right bottom. In this latter regard, the private information would be a digital number of 8,000 bits. At this point, the private information has been rendered (in a manner that is repeatable) into a digital object that may be processed in response to the information contained in the document 10.

Returning now to the document 10, an image 16 of the document is obtained by conventional means. In this regard, the Oxford Dictionary of Computing, Fourth Edition (1996) defines an image as "a copy in memory of data that exists elsewhere ...". Preferably the image 16 is a digital image that may be digitally Processed by well known, repeatable means to produce a digital representation of some feature of the image 16. For example, the digitizing element or step 18 may comprise processing according to the well-known ISO 10918 standard, with the product being an image feature such as spectral content, that may be represented by a rectangular array 19 of samples, with each sample being embodied in a digital number.

Without limiting the scope of my invention, another example may be considered. Assume that the document 10 is a video program and that the image 16 is a sequence of digitized video frames. Now, the digitization element Or step

18 could comprise an embodiment of the well-known ISO/IEC 11172 standard which compresses video images with associated audio and timing information. The output of the element or step 18 could be one, some, or all of the frames of the video in some predetermined repeatable sequence.

Up to this point, I have described how private information is received and rendered into a digital form that may be processed in response t0a digital form of some feature of the information contained in the document 10. Preferably, my invention provides for scrambling of the private information in the digital array 14 in response to the digitized image feature produced at 18. Preferably, scrambling is done in a linear feedback shift register (LFSR) 20 that is seeded by a l x n digital number embodying the digitized private information available in the array 14. In this regard "seeding" means initially loading the digital number into the LFSR 20 through its loading port (L). The LFSR 20 is a shift register of n-stages whose operation is controlled by sequence of clock pulses provided from the clock generator 22 to the clock port (C) of the LFSR 20. The operation of an LFSR such as the LFSR 20 may be understood with reference to Sklar's DIGITAL COMMUNICATIONS Fundamentals and Applications, Princess-Hall (1988), pp. 546-549. The LFSR 20 scrambles the digital number embodying the private information in a series of shifts, each shift occurring in response to a clock pulse produced by the clock generator 22.

The clock generator 22, whose operation is discussed in more detail below, operates in response to the array of samples produced by the element or function 18. When the array has been traversed, an END OF ARRAY signal is produced that disables the clock generator 22 and unloads the contents of the LFSR 20 by way of its output port (O). When the END OF ARRAY signal occurs, the operation of the LFSR 20 will have scrambled the digital number that embodies the private information in a pseudo-random manner. This process may also be referred to as "randomization" or "pseudo-randomization". The contents of the LFSR 20 are then arranged into an array 24 of ones and zeroes. Preferably,

the array is a two-dimensional matrix. As is known in the image processing art, a two-dimensional array of binary digits may be represented in a visual manner as a two-tone image formed by an array of pixels, with each pixel corresponding to a respective identically-located bit in the array of binary digits. In this regard, if rendered as a visually-perceptible image, the array would be black at each pixel location corresponding to a one in the array of binary digits, and would be no color or white at each pixel location corresponding to a zero in the array of binary digits. This two-toned pixel array is represented at 26. Assuming as per the example discussed above that the LFSR contains 8,000 binary digits, the arrays 24 and 26 would be approximately 90 bits x 90 bits in size, with a high degree of granularity in the image produced by the pixel array 26. It is possible to reduce the image of the pixel array 26 and append it as a mark 28 on the document 10. Now, the document 10 with the mark 28 included therein or thereon may be copied many times. It is possible that the process may reduce the resolution of the contents of the document 10, including the resolution of the mark 28. Ultimately; after production of a compounded number of copies, the mark 28 may be indecipherable. One way to increase the compound number of copies that may be made of the document 10 with the mark 28 on it is to reduce the granularity of the mark 28. This is accomplished in element or step 30 which operates on the pixel matrix 26 by distorting the image in a predetermined and repeatable way that results in a distinct mark having a coarser granularity than the pixel array 26. The product el the element or process 30 is referred to as a "blaze". The image of blaze is applied to the document at 32; the product being the document 10 on or in which the blaze 28b has been placed.

Certain details of the invention will now be discussed in greater detail. These details include the digital processing of the image 16, operation of LFSR 20, processing of the private information 11 and processing of the mark 28 to create the blaze 28b.

Referring to Fig. 2, assume that the document 10 is rendered into the

form of the electronic image 16. The image 16 may be represented by the image of Fig. 2, for example. This image may be processed to produce a compressed representation of a feature of the image. For example, the feature may be the image's spectral content. In this case, assuming processing according to the ISO 10918 standard, the image of Fig. 2 is subdivided into 8 x 8 non-overlapping tiles of pixels. Each tile is processed by application of a discrete cosine transform (DCT) which produces a digital representation of the tile. Each digital representation is quantitized and entropy-encoded. Next, each sample is compressed, with the compressed samples arranged into a rectangular array. The rectangular array represents a spectral content of the image. A representative array representing the spectral content of the image of Fig. 2 is shown in Fig. 3. Fig. 3 is a visual encoding of the spectral content; Fig. 4 illustrates the spectral content array of Fig. 3 in the form of a two-dimensional array of 16 bit digital numbers stored in the memory of a computer or processor. Each 16-bit digital number in the array of Fig. 4 corresponds to spectral content of an 8x8 tile of the original image of Fig. 2. The array of Fig. 4 corresponds to the array 19 produced by the element or step 18 of Fig. 1.

Refer now to Fig. 5 for an understanding of how the digitized image feature is used to clock the operation of the LFSR 20. In Fig. 5, the LFSR 20 includes a sequence of n registers 20r that are connected serially. The output of the right-hand register REG1 is fed back on a feedback path 20f in which linear arithmetic element 201 combines the output of the right-hand register REG1 with the output of an earlier register REGk. One or more linear arithmetic elements may be provided in the feedback path 20f. Fig. 5, for illustration only, shows an output of the feedback path 20f being provided to the input of the left-most register REGn. In response to a clock pulse input at the clock port C, the contents of the register array 20r are shifted one register position to the right. Scrambling of the register contents is produced by the one or more linear arithmetic elements in the feedback path 20f. The clock generator 22 produces clock pulses in

response to the contents of the array of 16-bit digital words represented by Fig. 4. The 16-bit digital numbers are fed sequentially to the input of the clock generator 22. The clock generator 22 embodies a process that determines the magnitude of a 16-bit digital number and then generates a clock pulse only if that magnitude exceeds some predetermined value. In this regard, assuming that the 16-bit number is unsigned, its magnitude may range in value from 0 (min) to a maximum value of $2^{16} - 1$ (max). In this case, the 16-bit digital number may have a mid-range value of 2^{15}. Assuming that the mid-range value is chosen as a threshold, each time a 16-bit number has a magnitude that exceeds the mid-range value, the clock generator 22 generates a clock pulse. On the other hand, no clock pulse is generated if the magnitude of the 16-bit number is less then the mid-range value. In order to ensure stability of operation, the clock generator 22 is invested with hysteresis. In this regard, if the last 16-bit number caused the generation of a clock pulse, then the following 16-bit number will generate a clock pulse so long as its magnitude is greater than 90% of the magnitude of the mid-range value. Similarly, if the last 16-bit number did not result in a clock pulse, then the following 16-bit number will produce a clock pulse only if its magnitude exceeds 110% of the mid- range magnitude.

In Fig. 6, an added level of security may be realized by subjecting the digitized private information 12 to an encryption process 13, with the output of the encryption process 13 seeding the LFSR 20.

The production of a blaze from a mark by "warping" or "smearing" the image of the mark is illustrated in Fig. 7. Assume, for the purpose of illustration, that the mark 28 comprises a 4 x 4 array of pixels. One way to decrease the granularity of the image of the pixel array 28 is to truncate each row by saving only the first two pixels and discarding the second two. In each row, each remaining pixel is doubled to produce the 4 x 4 image of the blaze 28b.

Fig. 8 illustrates an industrial application of my invention embodied in a computer system that includes a processing element 60, a user input element 62, a

document input element 64, and a document output element 66. The processing element 60 may be embodied, for example, as a process, a processor, an application specific integrated circuit (ASIC) or a programmed computer. The user input element 62 may include a mouse, a keyboard, or even a scanner. The user input element 62 is the means by which private information may be received by the processing element 60 from a user. The document input element 64 is the means by which a digitized image of the document 10 may be received by the processing element 60. For example, the element 64 may be a scanner, or a camera. The processing element 60 operates according to the explanation given in respect of Fig. 1 to produce a digital output that, when provided to the document output element 66, results in provision of the document 10 with either the mark 28 or the blaze 28b placed therein or thereon.

In this case assume that the element 66 is a printer. The document 10 may be the original of the document 10 with the printer printing the mark 28 or blaze 28b on the document itself, or the printer may reproduce the document 10 with the mark 28 or the blaze 28b. It should be realized that the complement of elements shown in Fig. 8 may be varied as appropriate for the medium and content of the document 10. Thus, for example, if the document 10 is a video, a VCR may be substituted for the scanner and for the printer.

Use of a mark or blaze according to the invention may be understood with reference to Figs. 9 and 10. In Fig. 9, assume that an image 80 with a mark 28 or blaze 28b on it is in hand and assume further that the provenance of the image 80 is known and traces to an original author of the image 80 whose private information resulted in creation of the mark 28 or the blaze 28b. Assume that an image 80r is received that is represented as an authorized copy of the image 80. Assume further that the image 80r contains a mark 81 that is purported to be derived from the private information of the original author of the image 80. The image 80r can be identified, authenticated, or otherwise validated as a copy of the image 80 by comparison of the images 80 and 80r, including their respective

marks or blazes. Comparison is done by an element 86 that employs a conventional image processing method to correlate the images and the marks or blazes. If the image 80r is a copy of the image 80, it is assumed that the images themselves will correlate within an error threshold (ε) input to the comparison process 86. Manifestly, the comparison will include correlation of the mark 28 or blaze 28b with the mark 81.

Another way in which to identify, authenticate, or otherwise verify the provenance of the document 80 is to use the private information from which the mark 28 or blaze 28b was derived. Using the private information 90 and the content of the document 80, exclusive of the mark or blaze 28 or 28b, a digital array representing a mark or a blaze is generated at 91. The compare element 86 uses the mark or blaze array generated at 91, digitizes the mark or blaze 28 or 28b in the document 80 and compares the two representations. If the element 86 can correlate the mark or blaze representation generated by 91 with the mark or blaze representation generated from 28 or 28b within the error threshold (ε), positive correlation (Y) will be indicated. Otherwise negative correlation (N) will be indicated.

Fig. 11 illustrates flow diagram that embodies steps of a computer-executed method embodying the invention. The method has two phases: generation, and validation. The generation phase includes steps 100, 102, 104, 105, 106, 107 and 108. The validation phase includes steps 110, 111,112, 114, and 116. The generation phase generates a mark or blaze in a manner corresponding with the illustrative description given earlier. Specifically, private information is received at step 100 and is processed at step 102 to create a digital representation of the private information. If desired, step 102 may include encryption. Alternatively, it should be realized that step 102 creates a number in digital form that represents the Private information input at 100. In step 104, the contents of a document are received; in step 105 the document contents are processed to generate a digital array representing a feature of the document

contents. For example, assuming that the document contents are an image, the array created in step 105 would represent the spectral content of the image input at 104. Alternatively, it should be realized that step 105 processes the document information to obtain a set, sequence, or array of digital numbers that represent the information in the document input at step 104. In step 106, the digital or numeric representation obtained in step 102 is scrambled in response to the digital or numeric representation of the document contents obtained in steps 105. In step 107, an image of the scrambled private information of step 106 is produced. The image may be the image of a mark. Alternatively, the mark image may be smeared to produce the image of a blaze. In step 108 the image of the mark or blaze produced in step 107 is placed on the document.

The inputs to the correlation phase may include the document imprinted in step 108. This document is input in step 110. Alternatively, the input to the correlation phase may be the private information originally input into the generation phase at step 100. In addition, a document with a mark or a blaze is inputted step 111. The document input in step 111 is to be identified, authenticated, or otherwise verified by either the private information or the document input at step 110. In step 112, it is assumed that all of the inputs are rendered into a digital or numeric form so that they may be correlated in a straightforward manner using known methods. Correlation is performed and tested against the error threshold ε. If less than the error threshold, the correlation validates the document input at step 111, taking the positive exit from step 112 to the validation indication at step 114. Otherwise, the correlation phase takes the negative exit from step 112, producing an invalid indication at step 116.

It should be manifest that the two phases of the method illustrated in Fig. 11 can be implemented in the same or separate processing machines. For example, it is contemplated that a machine that produces document copies by a photostatic process could incorporate the generation phase for generating of a mark or a blaze and marking documents. The same machine may also have the correlation

phase incorporated into it in order to test the validity of documents. In fact, it is contemplated that either or both of the marking and correlation functions may be incorporated into copy machines, digital cameras, processing machines or systems that incorporate or connect to printers, scanners, facsimile machines, and the Internet, CD manufacturing and playing machines, tape machines, VCRs, and so forth. Also, either or both of generation and correlation phases could be incorporated into many systems that archive, index, or otherwise process documents such as electronic libraries/museum systems, electronic verification systems, driver's license verification systems, passport verification systems, ID card/credit card verification systems, and so forth.

Further, the method of Fig. 11 in either or both of its phases could be implemented as a software program or routine stored in a memory or storage device or present in a network mode for programming a programmable device such as a processor or computer, or could be embodied in the electronic architecture of an electronic circuit or system composed of discrete parts or incorporated into one or more integrated circuits.

My invention also concerns a method and an apparatus for identifying an image based upon information in the image that is derived but distinct from the contents of the image itself. The information is either apprehended or entered in the image contents by correlation of the contents of an image of a uniquely-generated mark with the image contents of a succession of portions of the image. Accordingly, understanding of my invention requires first an understanding of how a mark or an image of a mark may be uniquely generated. It can be accomplished by referring to the earlier description made in connection with Figures 1 to 7, and regarding the reference to a document 10 as being made to an image 10.

Derivation of an image signature is now described in the following with reference to Fig. 12 wherein the image of Fig. 2 is separated into a plurality of image portions ("tiles"). Tiles generally are uniform subdivisions of an image,

having the dimensions of the image, but being smaller than the image itself. Typically, for an image I (xy) having a width W and a height H, the tiles Tij (x,y) will, upon superposition, form the complete image I (x, y). Fig. 12 shows how the image 10 (corresponding to the image in Fig. 2 or its transformation in Fig. 3, for example) can be subdivided into a plurality of tiles by scanning a tile-shaped window over a map of the image in a raster fashion, from the upper left-hand corner in a succession of scans preceding from the left to the right margin of the image. Scanning does not necessarily have to follow the raster format; the only requirement is that the scanning pattern be consistent and repeatable. Processing of the image according to the invention is by means illustrated in Fig. 13.

In Fig. 13 a map 30 of the image 10 is created, the map being a digital representation of the image in a memory that can be accessed by a tiling function 31 to provide a succession of tiles obtained by some regularized, systematic scanning of the image 10 using a tile window. A mark (or blaze) is generated as described above by the mark generator 32 in response to the image map 30 and personal information embodied, for example, in a personal identification number (PIN). The mark is provided at 33 to a correlation process 34, as is each tile 31 in the succession of tiles from the image 10. The correlation process 34 may comprise any of a known number of correlation processes including straight map correlation, linear correlation, exponential correlation, least squares correlation, and so forth. A number having a magnitude representing the degree of correlation between the mark 33 and the current tile 31 is output by the correlation process 34.

It should be understood that the mark that is input to the correlation process 34 is, more properly, an image of the mark (which may be an image map stored at 33), whose contents are rendered in the same form as the contents of each tile 31. Thus, in the correlation process 34, the image content of the mark 33 is compared with the image content of the current tile in the succession of files. The correlation process 34 determines a degree of similarity between the image

content of each tile and the image content of the mark 33, which similarity can be expressed as the magnitude of a number. The mark 33 (or blaze) preferably has a dimensional format that is consistent with the format of the tiles in shape and size. This does not mean that the mark should or must have a size and/or dimensions that are identical to those of the tiles. The requirement is that the mark be of a size and shape that permit its image contents to be correlated with the image content of the files. A data structure is established and filled by the correlation process 34. The data structure (represented by a correlation map 36) contains, for each file, the magnitude of the number generated by the correlation process 34 that represents the degree of correlation and therefore the degree of similarity between the image content of the tile and the image content of the mark. In the correlation map 36, degrees of similarity are indicated for four files, denoted as A, B, C, and D.

The correlation map 36 represents information that is related to, but distinct from the content of the image 10. A signature for the image 10 is derived or apprehended from this information by means illustrated by the block diagram of Fig. 14. In Fig. 14, the correlation map 36 is accessed by a signature extraction function 38. The signature extraction function 38 establishes a threshold 37 to determine a unique signature for the image 10. The threshold 37 represents a threshold above which similarity magnitudes are encoded to derive a unique signature for the image 10. In this regard, an encoding scheme generates a signature from the similarity measures that exceed the threshold 37. One such scheme may provide, for example, binary encoding of successive pairs of similarity measures that exceed the threshold. In this regard, a zero is generated if the magnitude of the first measure exceeds the magnitude of the second measure. For example, the pair of similarity measures for tiles A and B both exceed the threshold 37 and the magnitude of the first measure (for tile A) exceeds the magnitude of the second measure (for tile B), resulting in the encoding of a zero. For the next pair of measurements whose magnitudes exceed the threshold 37, the

first (for tile C) is exceeded by the second (for tile D), resulting in encoding of a one. In this manner, a succession of pairs of similarity measures can be used to apprehend or extract a digital signature that identifies the image 10. A string of such pairs is stored at 39, and encoded at 40, and an encoded signature is received in a signature buffer 41. In the buffer 41, the signature is represented by a succession of binary digits, the first of which is zero, the second of which is one, and so on.

Manifestly, those skilled in the art will appreciate that the set of magnitudes that exceed the threshold 37 comprise an unencoded string that may be mapped into a symbol alphabet by any appropriate coding scheme. In Figs. 13 and 14, the alphabet is binary and the coding scheme maps two elements of the unencoded string to one binary element of an encoded string, wherein the encoded string is a signature of the image 10. This example is not meant to limit signature generation to two-to-one encoding, or to binary encoding; in fact, other coding schemes may be used.

Fig. 15 illustrates an alternative embodiment of signature derivation for the image 10 in which the image content of tiles in the succession of tiles fed to the correlation process 34 can be altered by algebraic combinations (addition or subtraction) of the image content of the mark 33 with the image intent of one or more tiles. In this manner, a pattern insertion function 42 is provided with the similarity measures generated by the correlation process 34 and with the current tile that is being input to the correlation process 34. The pattern insertion function 42 also receives the image of the mark 39 and either knows or receives a code for a desired signature 43. The pattern insertion function 42 operates to impose an encoding on the correlation results produced by the correlation process 34, thereby to alter or change the image content of the image at corresponding tile locations in order to weave or insert a desired signature 43 into the image 10. In order to minimally disrupt the image, the pattern insertion function 42 alters the image content of the image map 30 at the current tile location only if the

correlation between that image content and image content of the mark meets or exceeds a threshold and then only if such alteration is necessary to insertion of the signature. In this manner, the alteration of the image 10 can be made virtually imperceptible to the human eye but tractable to a machine.

For example, with reference to Fig. 15, the pattern insertion function 42 may impose an encoding threshold 43 in the magnitudes of correlation results such that the magnitudes for tiles A, B, C, and D (and so on) exceed the threshold. The signature 43 may then be inserted by changing the correlation result of one or more tiles, which is accomplished by adding or subtracting the image content of the mark to the image map 30 at the corresponding tile location or locations. In this regard, presume that the correlation result at Tile A is indicated by 44, wherein the magnitude of the result is greater than that at Tile B. Presume also that the magnitude of the correlation result in Tile C is indicated by 46, which is greater than the result for Tile D. Presume that Tiles A, B, C, and D are to be encoded to achieve the result described in connection with Figs. 13 and 14. The result requires that the unencoded string A, B, C, D be encoded by adding some degree of the image content of the mark to the image content at Tile A to increase the correlation result by the amount 47 and by subtracting some amount of the image content of the mark from the image content at Tile C to reduce the correlation result by the amount 48. Then, the string A, B, C, D is encoded as described above.

Fig. 16 illustrates a process for generating a unique identification for the content of an image (such as the image 10) using the description given above in connection with Figs. 13 and 14, which illustrate what may be termed an "extracting" process and in connection with Fig. 15 which illustrates what may be termed an "inserting" process. Initially, in step 53, an image such as the image 10 is rendered in a grey scale representation in the form of an image map that may reside in the memory of a computer. Grey scale conversion is not a necessary prerequisite for practice of my invention, nor is it the only way of representing

the content of an image. It is simply an example of one convenient way to access the content of an image. Using a conventional image processor in the form of a software program executed by the computer, the image map may be tiled with the tiles being fed in some predetermined sequence to the main memory of the computer. Thus in step 54, the next tile in the sequence is placed in the main memory and there provided to a correlation process executing in the CPU of the computer in step 55 where the image content of the current tile is correlated with the image content of the mark 56. If the process uses the extraction mode of signature derivation, the "extraction" exit is taken from the decision 57 and the magnitude of the correlation between the current tile and the mark is entered into a correlation map in step 58. If no more tiles remain (decision 59), a threshold is applied in step 60 to the correlation map to derive an unencoded string. In step 61 a code representing the signature is derived from the unencoded string and the signature is stored, or output, together with the mark 56 in some persistent storage medium accessible to the user (human, machine, or process) who initiated the process.

If the insertion mode is being utilized, the "insertion" exit is taken from decision 57 and decision 62 is entered where the correlation magnitude for the current tile is compared with an encoding threshold 63. If the magnitude falls below the encoding threshold 63, the process returns to A; otherwise, in decision 64, for the next symbol of the signature to be produced, the decision is whether to adjust the image content of the current tile as required to produce the next symbol of the signature 65. If not, the procedure returns to A. Otherwise, the image content of the mark is added or subtracted to the image content of the image map at the location of the current tile in step 66 and the process enters decision 67. If more tiles remain, the process returns to A; otherwise the positive exit is taken from decision 67 to step 68. In step 68, with no tiles remaining, the signature inserted in the image is stored, with the mark 56 in some persistent storage medium accessible to the user (human, machine, or process) who initiated the

process.

Fig. 17 illustrates an industrial application of my invention embodied in a computer system 75 that produces copies of an image, The system 75 includes a processing element 78 with a memory 79, storage 80, a user input element 82, an image input element 84, and an image output element 86. The processing element 78 may be embodied, for example, as a process, a processor, an application specific integrated circuit (ASIC) or a programmed computer. The user input element 82 may include a mouse, a keyboard, or even a scanner. The user input element 82 is the means by which private information (a personal identification number -PIN- for example) may be received by the processing element 78 from a user. The image input element 84 is the means by which a digitized image of an original image may be received by the processing element 78. For example, the input element 84 may be a scanner, or a camera. The processing element 78 operates according to the explanation given above to produce a digital mark and to derive a signature for the image 99. For this explanation, it will be assumed that the image 99 is on a document 100, and that the system 75 includes a document processing component. Thus, the output element 86 may produce a copy 99c of the image rendered in a copy 101 of the document 100. In this case it may be assumed that the element 86 is a printer.

Referring now to Fig. 17, assuming processing of the image 99 according to either of the extraction or the insertion processes described above, the processing element 78 using the resources 79, 80, 82, and 84 derives a unique mark and a signature for the image 99. The mark and the signature for the image 99 are stored in a table 90 (or file, or other equivalent structure), in persistent storage 80 (such as a direct access storage device--DASD), together with an indication of when the mark and signature were entered into the table 90. This indication can comprise, for example, a date/time stamp (DS). In this example, the system 75 can provide to a user a persistent storage medium bearing the mark, signature, and date/time stamp generated for the image 99. In some instances, the

persistent medium might include the document 100 itself, or in addition to another persistent medium. Such operation is useful, for example, in the case where the user has created the image 99, the original of which is carried on the document 100. A copy of the image can be submitted for copyright registration in which the mark/signature/DS information would be entered into a relevant field of the copyright registration application form. This would enable the originator of the image 99 to submit for pubic recordal information respecting identification of the image 99 that could be used to establish the provenance of the image 99.

With respect to the insertion process, the system 75 illustrated in Fig. 17 would render the image 99 on the document 100 in one or more copies 99c of the image on one or more documents 101. Of course, each copy 99c would have the signature inserted into it, which would enable the system 75 to identify, authorize, or otherwise validate Copy 99c in response to the same PIN that originated the signature. In this case, the extraction process would be useful to obtain the signature of the image copy 99C. The signature could be used, for example, to link the original image 99 and all of its copies 99c to an enterprise that owns one or more systems 75, to the specific system 75 that created the copies, or to a set or a database of proprietary documents.

Fig. 18 shows an inverse process for checking a signature apprehended in an original image 149. Presume that the image 149 and PIN 150 have previously been provided to an extraction process and that an original mark 152o and signature 153o have been derived from the image and provided on a persistent storage medium. Now the image 149 and the PIN 150 are provided to a decoding process 151 that may be the equivalent of the extraction process described above. In response to the image 149 and the PIN 150 decoding process 151 generates a mark 152 and, in response to the mark, apprehends a signature 153. A comparison function 155 receives the mark/signature pairs and provides an output (Y/N) indicating whether or not the pairs are equivalent.

An alternate way of validating either an original image 149 or a copy

149c of the original image (with a signature inserted therein) is to use the decoder 151 as explained in connection with Fig. 19. The decoder 151 receives the image 149 (or copy 149c) and PIN 150, generating therefrom a mark and a signature either inherent in the image 149 or inserted earlier into its copy 149c. The decoder 151 provides the mark as an index into a table 190 (or a file, on other equivalent structure) such as the table 90 in which mark/signature/DS tuples are stored. The index outputs a particular tuple from the table 190 to a compare function 155 that compares the tuple with the output of the decorder 151 to identify, validate, and/or otherwise authorize processing of the image 149 (or copy 149c).

It should be manifest that the signature derivation modes illustrated in Fig. 16 and the checking procedures of Figs. 18 and 19 can be implemented either alone, or together, in the same or separate processing machines. For example, it is contemplated that a machine that produces document copies by a photostatic process could incorporate the insertion mode for placing a signature in an image copy. The same machine may also have the correlation procedure of Fig. 19 incorporated into it in order to test the validity of one or more copies made from the same image. In fact, it is contemplated that one or more of the signature derivation and checking functions may be incorporated into copy machines, digital cameras, processing machines or systems that incorporate or connect to printers, scanners, facsimile machines, and the Internet, CD manufacturing and playing machines, tape machines, VCRs, and so forth. Also, one or more of signature derivation and checking phases could be incorporated into many systems that archive, index, or otherwise process image-bearing documents such as electronic libraries/museum systems, electronic verification systems, driver's license verification systems, passport verification systems, ID card/credit verification systems, and so forth.

Further, the method of Fig. 16 in either or both of its modes and either or both of the checking procedures of Figs. 18 and 19 could be implemented as a

software program or routine stored in a memory or storage device or present in a network node for programming a programmable device such as a processor or computer, or could be embodied in the electronic architecture of an electronic circuit or system composed of discrete parts or incorporated into one or more integrated circuits.

My invention additionally concerns a method and a system, apparatus, or appliance for hiding information in the text of a document, based upon scrambling private information in response to information in an image of the document.

Fig. 20 is a block diagram organized to illustrate the functional components and operational flow of the system and a process that uniquely hides information in the text of a document such that the hidden information is imperceptible to sight, yet tractable to a machine so that the information may be extracted from the text and used for various purposes, such as identifying the document. Consider initially a document 112 containing text. For the purposes of this invention, the document may be entirely text or it may contain portions of text together with other portions containing other visual information such as graphics and/or images. The text may include characters, letters, numerals, symbols, and punctuation marks, and so on. The text may implicate any system of written language. The invention contemplates that these characters, contained in a document, may be manipulated individually or collectively by a computer operating on a digital image of the document. As those skilled in the art will appreciate, when the document 112 is rendered into the fob-m of a digital image, the structure of the text it contains can be derived using conventional means that are known, for example, in the construction and operation of optical character readers or scanners. Further, each character in the image can be decomposed into constituent parts which, for convenience, are termed "text kernels" in this description. Thus, any character set can be decomposed or deconstructed into a set of text kernels and any character of the character set can be constructed by

assembling text kernels in the set of text kernels. For example, consider the letter T in the English alphabet. In a text processing system, the letter will be constructed in a letter "cell" in a bit map representing a digital image of a document containing the letter. In this cell, the letter would be constructed using a text kernel consisting of a single horizontal line positioned at a location in the upper third of the cell, and a text kernel consisting of a longer vertical line positioned underneath and between the ends of the horizontal line.

The invention is based upon the realization that text kernels in the text of the document can be accessed and their positions, or the positions of the letters that contain them, can be altered slightly in a regular fashion that results in the encoding of information. The encoding can be virtually imperceptible to human sight if it is limited to shifting text character positions by only a few pixels and by imposing the same shift on a run of characters containing the same kernels as they are encountered in scanning lines of text. By limiting the change of position to very small distances - measured in five or fewer pixels, for example, a visible manifestation of the document such as on the screen of a computer system or in a printed hard copy will be difficult if not impossible to detect with the human eye. Further, by imposing the limitation of a position of the same adjustment on a run of characters containing a common image kernel, very slight character-to-character variations and location will be even harder to detect visually.

Accordingly, in Fig. 20, the document 112 containing text (hereinafter "text document") is input into a computer system by conventional means, for example, by an optical character reader or scanner. As those skilled in the art will appreciate, an appliance such as an optical character reader or a scanner will create a digital image of the document, with the lines of text positioned with reference to a known frame of reference. In this regard, the lines of text will be identified by their start points and end points, by their horizontal center lines, and so On. The output of such an appliance is a digital image of a document which is referred to hereinafter as "document image" 114. The digital image is represented

by a bit map. A tiling function ("tiler") 116 is employed to at partition the document image into an array of non-overlapping tiles. One such tile is indicated by reference numeral 118. The tiles of the array are accessed in a sequence that can be a regular scanning sequence proceeding, for example, from the top left portion of the document image to the bottom right portion. This is not a necessary constraint; the tiles can be accessed in any order that is known and repeatable. Preferably, however, the sequence of tile access that is known to a system authority having control over the configuration, operation, and administration of the system. Each tile of the document image is transformed into digital form, producing a digital signal that is fed to drive a clock generator 120. The conversion of each tile produces a digital number that is identical to the digital number produced by a later conversion of the same tile by the same conversion process. Thus; using the same conversion process, success of conversions of the same tile will cause the clock generator 120 to generate an identical number of clock pulses for each conversion of that tile. The clock pulses produced by the clock generator 120 in response to a digital number representing a tile of the document image clock a linear feedback shift register (LFSR) 122 that is initially seeded by digital word representing private information 124 that is known only to the system authority. The LFSR 122 operates conventionally to randomize or pseudo randomize the seed in response to the output of the clock generator 120. This is also referred to as "scrambling". Thus, the digital word derived from each tile and the succession of files produced by the tiler 116 causes the clock generator 120 to produce the corresponding set of clock pulses that cause the LFSR 122 to scramble its contents.

The provision the of a succession of tiles therefore causes the LFSR 122 to produce a succession of digital words. From each digital word, an index is derived that is provided to a coder 126. The coder 126 uses an index to obtain a page of a code book 128. Each page of the code book 128 contains a text kernel. The coder 126 using the text kernel currently indexed, encodes information 125

in the text contained in the document image in such a manner as to keep the information 125 hidden, at least to the eye. The coder 126, operates on the characters of the text that contain the text kernel of the currently indexed code book page. When coding is complete, the document image with encoded text at 30 is provided to an output appliance that outputs the document with encoded text at 32.

Those skilled in the art will appreciate that the architecture of Fig. 20 can be incorporated in whole or in part into a programmed, general purpose digital computer, a special digital processor, an application specific integrated circuit (ASIC), a server, a network node, and so on. Manifestly, the architecture of Fig. 20 could incorporate the code book 128 as a securely programmed read only device, as a securely reprogrammable device, or any equivalent.

Fig. 2 illustrates the data structure of the code book 128 shown in Fig. 20. This data structure is representative and illustrative, and may be varied as required for any particular implementation. The code book 128 includes a code table 200 having a plurality of columns. One column is an index column containing a number to which the index derived from the current contents of LFSR 122 maps. A second column includes an identification of a code page (code page i). Each entry in the code page column points to a code page, such as the code page 206. Code page 206 contains a representation identifying a text kernel; this is illustrated, for example, by the text kernel 208.

Fig. 22 illustrates a document 300 with lines of text, such as the line 302. The line of text in the document 300 contains characters such as the H 305 arranged to convey or signify information, for example, the text line 302 contains text that includes the words: THIS TOO TOO SOLID ..., In this line of text, there are a plurality of occurrences of the character T, three of which are indicated by 310, 311 and 312. This character comprises two text kernels, the horizontal and vertical text kernels described above. Presume that the text kernel 208 currently indexed via the table 200 in Fig. 21 corresponds to the horizontal portion of the

letter T. Information may be hidden in the document 300 by an encoding process that accesses each of the occurrences of T in the document 300 and encodes them in some fashion. For example, presume that there are 100 occurrences of T in the document 300 and that a binary character, such as a one is to be hidden in the document 300. In this case, an exemplary coding scheme using the character T might change the location of some or all of the occurrences of T in the document 300. As an illustration, presume that encoding a one is accomplished by moving the first 40 percent of the occurrences of T in the document 300 in a first direction and the last 40 percent of the occurrences in the opposite direction, with the middle 20 percent left in their original positions or centered with respect to the centers of the lines in which they are contained. In this regard, conventional means exist to determine the statistical center of each of the lines of the document 300 and to adjust the locations of selected characters or portions of the characters in those lines. Continuing with the example based on the character T, Fig. 23 illustrates how the character might be represented in a bit map 400 wherein each of the text kernels is represented by an array of pixels. Thus, the image kernel 208 is represented for each instance of the character T by the upper horizontal array 401 of pixels in the illustration presented in Fig. 23. For hiding information by coding the T's, the first 40 percent of the T's could be moved in a first direction such as up or down (indicated by the arrows 402a and 402b), left or right (403a, 403b) and so on. Preferably, the movement of the characters is by a few pixels' distance in the first direction. Further, the direction of movement is with respect to the statistical centerline of the line of text where the character is located. Continuing with the example, presuming 100 T's in the document 300, the first 40 T's would be moved in the direction of the arrow 402a by, say, two pixels' distance away from the centerline, the last 40 T's by an equal amount in the opposite direction from the centerline, while the middle 20 T's are moved to a central position between the first and last 40 occurrences.

It is not necessary that each character in the run of characters be moved.

The invention contemplates coding by movement or alteration of the text kernels alone, instead of the characters in which they are found.

Coding may proceed in this or any equivalent manner for so long as it is necessary to hide the identifying information in the document 300.

Fig. 24 is a flow diagram representing a computer program embodying or otherwise implementing a procedure according to the invention. Initially at 500, the system of Fig. 20 is initialized with the private information 124, the information 125 that is to be hidden, and a text document. In step 502, the LFSR 122 is seeded with the private information and the text document is scanned in, oriented, and rendered as a digital image in, for example, bit map form. The document image is then partitioned into tiles, with the tiles taken in the desired sequence. For the next tile in the sequence, obtained in step 503, the tile is converted into digital form, with the digital form driving the clock generator 120 for a period of time or for the generation of a number of pulses that is determined by the digital value of the digital representation of the tile. This operates the LFSR 122, causing it to scramble its contents in a random or pseudo random manner. When the current operation of the clock generator 120 in response to the digital representation of the current tile is completed, an index is generated from the contents of the LFSR in step 504. The index is provided to the coder 126 which accesses the code book 128 to obtain a code page with a text kernel. The coder 126, using the text kernel encodes some portion of the information to be hidden into text characters having the indexed kernel in step 506. In step 507, the process executes a decision with respect to whether the entire information 125 to be hidden in the text has been encoded. If not, the negative exit is taken and the sequence 503, 504, 505, 506, 507 is again executed. Otherwise, the document image with encoded text containing the hidden information is output in step 508. The loop through the negative exit of the decision 507 presumes that the information to be hidden in the text consists of a set or string of bits or symbols that have to be encoded in some sequence.

Decoding of information hidden in text of a document according to this invention presumes that the hidden information is coded by moving characters, moving text kernels, or altering text kernels in the text in such a manner that characters or text kernels can be identified by the components of Fig. 20 and the steps of Fig. 24 that produce an index using the LFSR 122. Extraction of the hidden information requires generation of a document image and input of the same private information used to encode the document with the hidden information. This will permit a decoder to identify the sequence of characters (or text kernels) that were used to place the hidden information in the document as described above. Once the characters (or text kernels) and their sequence are known, decoding straightforwardly precedes by detecting patterns in the variations of the locations of the sequence of characters (or text kernels) with respect to the centerlines of the lines of text in which they are contained. Clearly, the other embodiments and modifications of this invention will occur readily to those of ordinary skill in the art in view of these teachings. Therefore, this invention is to be limited only by following claims, which include all such embodiments and modifications when viewed in conjunction with the above specification and accompanying drawings.

CLAIMS

1. A computer-executed method of processing information of a document to create an identification mark, comprising:

receiving private information;

processing the private information to obtain a numeric representation of the private information;

processing the document information to obtain a numeric representation of the document information;

seeding a randomizer with the numeric representation of the private information;

causing the randomizer to scramble the numeric representation of the private information in response to the numeric representation of the document information; and

producing an image of the scrambled private information.

2. The method of claim 1, wherein processing the private information includes encrypting the private information.

3 The method of claim 1, further including placing the image of the scrambled private information on the document.

4. The method of claim 1, wherein the image of the scrambled information has a granularity, the method further including producing a blaze by reducing the granularity of the image of the scrambled private information.

5. The method of claim 4, further including placing the blaze on the document.

6. The method of claim 5, wherein the blaze is placed substantially apart from the information of the document.

7. The method of claim 1, wherein the scrambler includes a linear feedback shift register (LFSR).

8. The method of claim 7, wherein causing the randomizer to scramble includes clocking the LFSR in response to the numeric representation of the document information.

9. The method of claim 8, wherein processing the private information includes encrypting the private information.

10. The method of claim 8, wherein the image of the scrambled information has a granularity, the method further including producing a blaze by reducing the granularity of the image of the scrambled private information.

11. The method of claim 10, further including placing the blaze on the document.

12. The method of claim 1, wherein the numeric representation comprises a digital representation.

13. A program product including a storage medium and executable instructions stored in the medium for processing information of a document to create an identification mark according to the method set forth in claim 1.

14. A device for processing information of a document to produce an identification mark in response to private information, comprising:

first means for providing a first digital representation of the private information;

second means for providing a second digital representation of the document information;

a randomizer for scrambling the first digital representation in response to the second representation to produce a third digital representation of scrambled private information; and

third means for providing an image of the third digital representation.

15. The device of claim 14, further including means for encrypting the private information, the first means for scrambling encrypted private information.

16. The device of claim 14, further including fourth means for changing the granularity of the image of the third digital representation.

17. The device of claim 14, wherein the randomizer is a linear feedback shift register.

18. A device for processing information of a document to create an identification mark, comprising;

first means for providing a first numeric representation of the private information;

second means for providing a second numeric representation of the document information;

a randomizer for scrambling the first numeric representation in response to the second numeric representation to produce a third numeric representation of scrambled, private information; and

third means for providing an image of the third numeric representation.

19. The device of claim 18, further including means for encrypting the private information, the first means for scrambling encrypted private information.

20. The device of claim 18, further including fourth means for changing the granularity of the image of the third digital representation.

21. The device of claim 18, wherein the randomizer is a linear feedback shift register.

22. A method for identifying an image using electronic means, comprising:

receiving an image in electronic storage;

receiving personal information in the electronic means;

generating a mark by combining contents of the image with the personal information;

producing information by comparing an image of the mark with a plurality of portions of the image; and

deriving a signature uniquely identifying the image from the information.

23. The method of claim 22, wherein deriving the signature includes apprehending the signature in the information.

24. The method of claim 23, wherein deriving the signature further includes correlating image contents of the mark with image contents of each of the plurality of portions and producing correlation results and apprehending includes applying a threshold to the correlation results to produce a candidate string and encoding the candidate string.

25. The method of claim 22, wherein deriving the signature includes inserting the signature into the image.

26. The method of claim 23, wherein deriving the signature further includes correlating image contents of the mark with image contents of each of the plurality of portions and comparing the results of correlating with a threshold, and inserting includes altering the contents of the image at one or more locations when the correlation of those contents with the image contents of the mark exceed the threshold.

27. The method of claim 22, further including storing the mark and the signature in a persistent storage medium.

28. The method of claim 27, wherein the image is on a document and the method further includes storing the signature on the document, apart from the image.

29. The method of claim 23, further including verifying the image by:

receiving an image in electronic storage;

receiving personal information in the electronic means;

generating a second mark by combining contents of the image with the personal information;

producing second information by comparing an image of the mark with a plurality of portions of the image;

deriving a second signature from the information;

comparing the signature with the second signature; and

validating the image if the signature is identical to the second signature.

30. The method of claim 25, further including: receiving an image in electronic storage;

receiving personal information in the electronic means;

generating a second mark by combining contents of the image with the personal information;

producing second information by comparing an image of the mark with a plurality of portions of the image;

deriving a second signature from the information; comparing the signature with the second signature; and

validating the image if the signature is identical to the second signature.

31. The method of claim 30, wherein the second step of receiving an image includes receiving a copy of the image.

32. A system for identifying a image, including:

means for receiving an electronic image;

means for receiving personal information;

means for generating a mark by combining contents of the electronic image with the personal information;

means for producing information by comparing an image of the mark with a plurality of portions of the image; and

means for deriving a signature uniquely identifying the image from the information.

33. A system for hiding information in text contained in a document, comprising:

means for producing an index by scrambling private information in response to a digital image of the document; and

a coder that adjusts locations of characters in the text of the document in response to the index.

34. The system of claim 33, wherein the coder includes a code table that

indicates text kernels.

35. The system of claim 34, wherein the code further includes code pages and the text kernels are contained in the code pages.

36. The system of claim 35, wherein the hidden information is coded in the locations of the characters that are adjusted by the coder.

37. The system of claim 33, wherein the hidden information is coded in the locations of the characters that are adjusted by the coder.

38. The system of claim 33, wherein the coder adjusts locations of portions of characters in the text of the document in response to the index.

39. A method for hiding information in text contained in a document, comprising:

producing an index by scrambling private information in response to a digital image of the document; and

coding the information in the text by adjusting locations of characters in the text of the document in response to the index.

40. The method of claim 39, wherein coding includes indexing into a code table.

41. The method of claim 40, wherein indexing includes indicating a text kernel and coding includes adjusting locations of characters that contain the text kernel.

42. The method of claim 39, wherein coding includes indexing to a text

kernel and coding includes adjusting locations of characters that contain the text kernel.

43. The method of claim 42, wherein coding includes indexing to a succession of text kernels.

44. The method of claim 39, wherein coding the information in the text includes adjusting locations of portions of characters in the text of the document in response to the index.

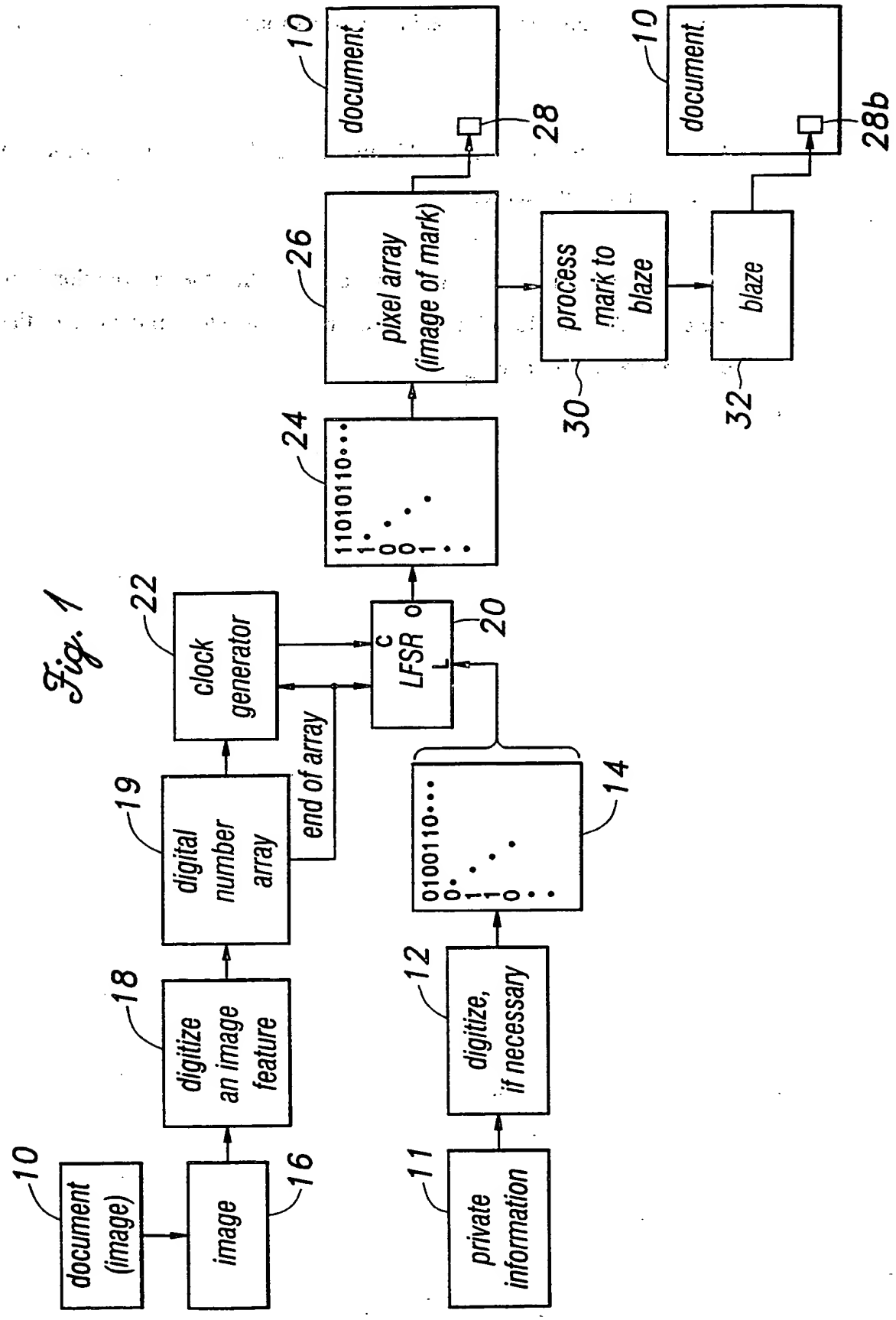

document (image)
10
image
16
digitize an image feature
18
digital number array
19
clock generator
22
end of array
private information
11
digitize, if necessary
12
0100110...
14
LFSR
20
11010110...
24
pixel array (image of mark)
26
document
10
28
process mark to blaze
30
blaze
32
document
10
28b

Fig. 1

Fig. 2

Fig. 3

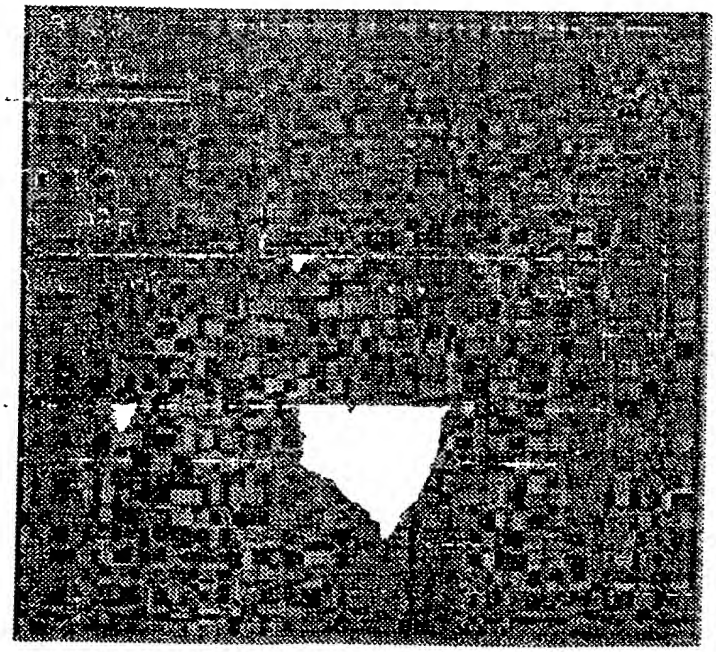


Fig. 4

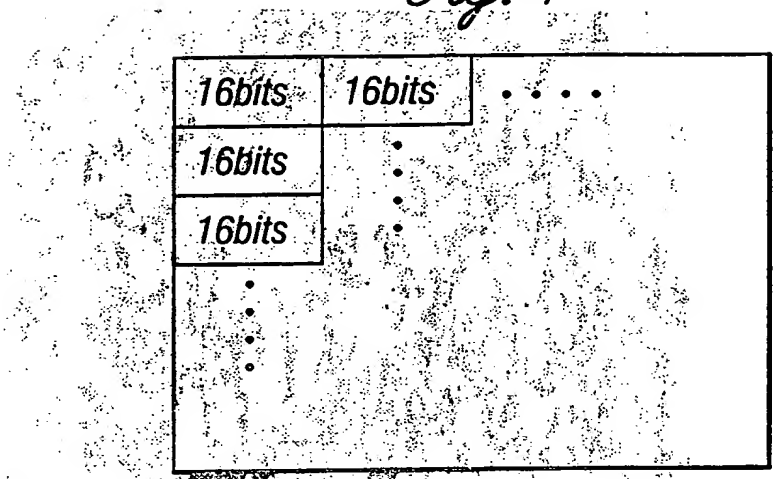


Fig. 5

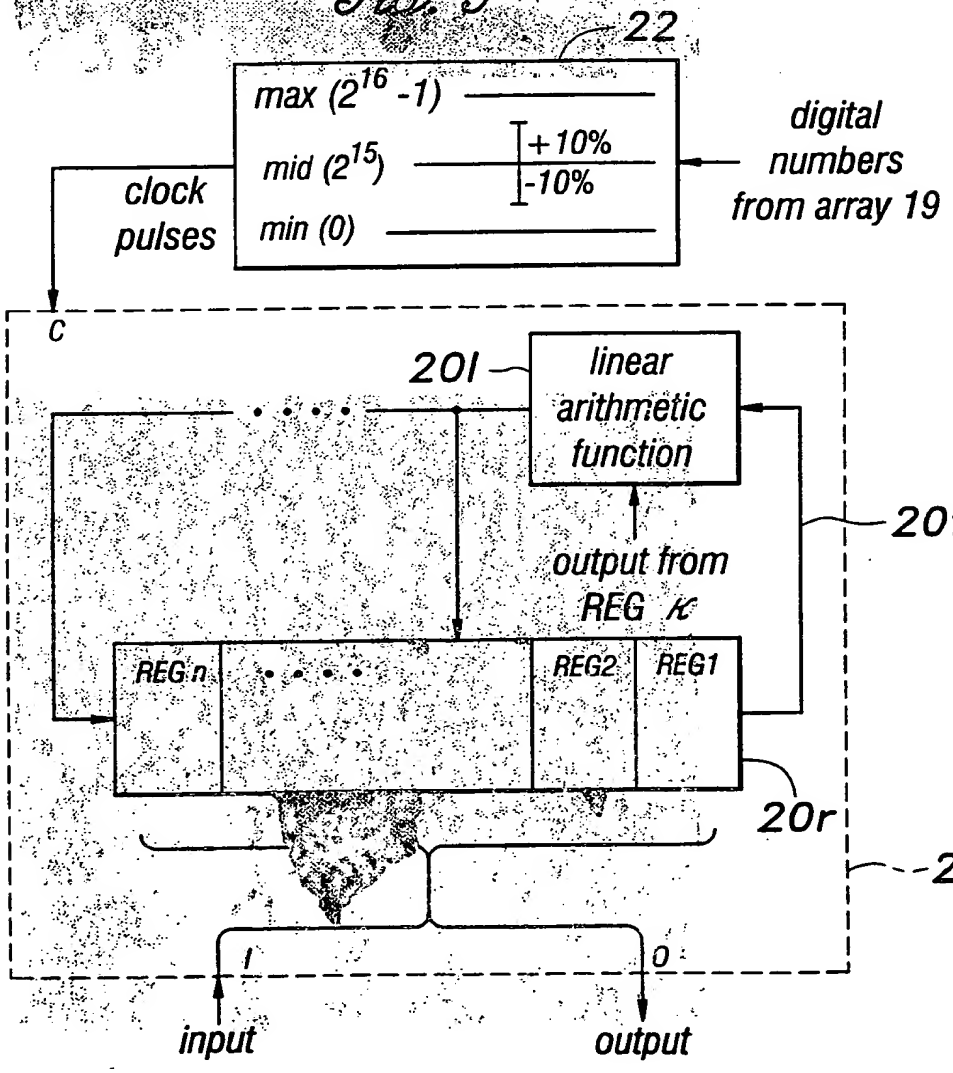


Fig. 6

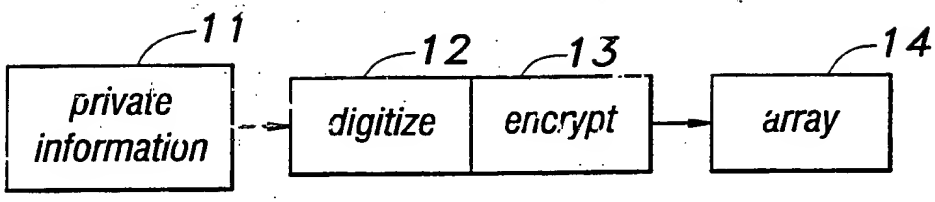


Fig. 7

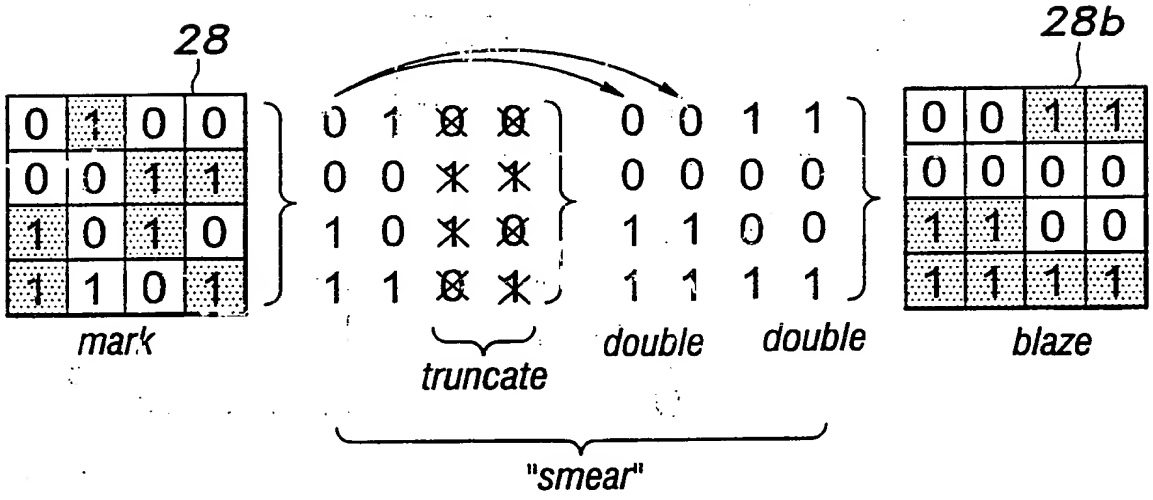


Fig. 8

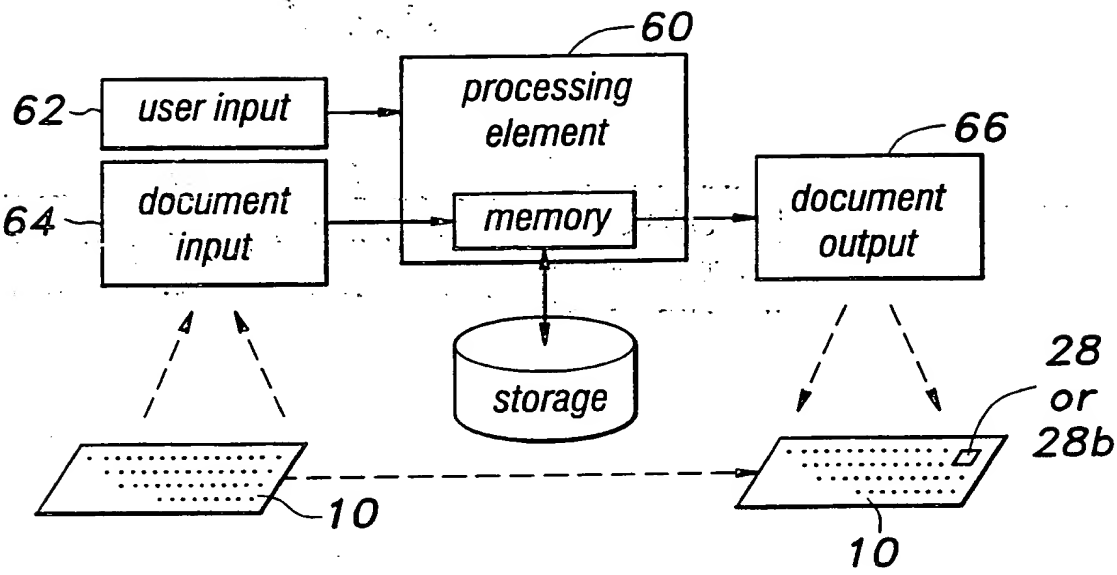


Fig. 9

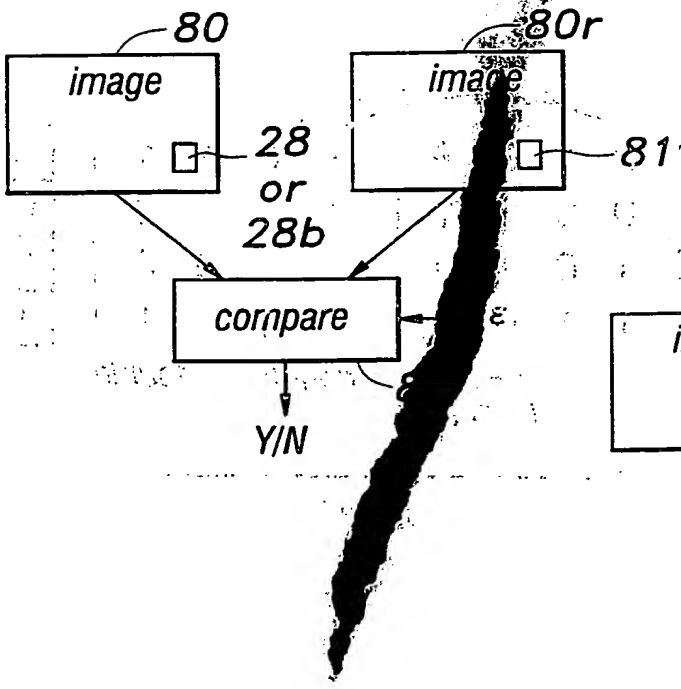


Fig. 10

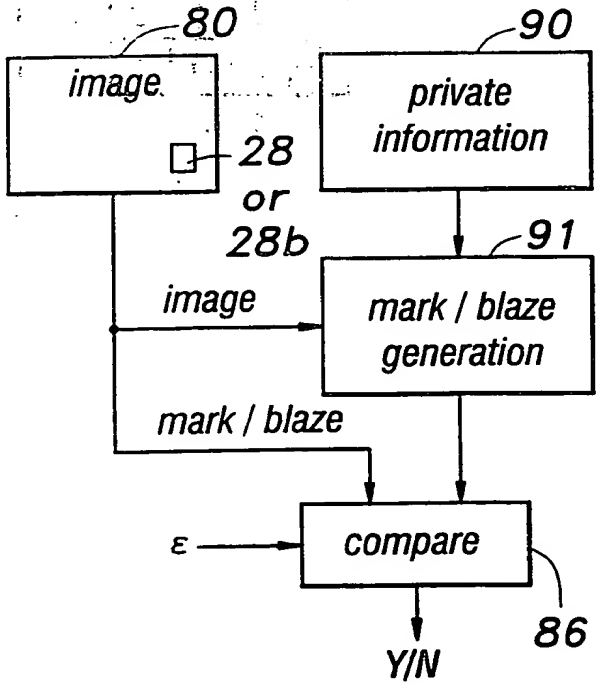


Fig. 11

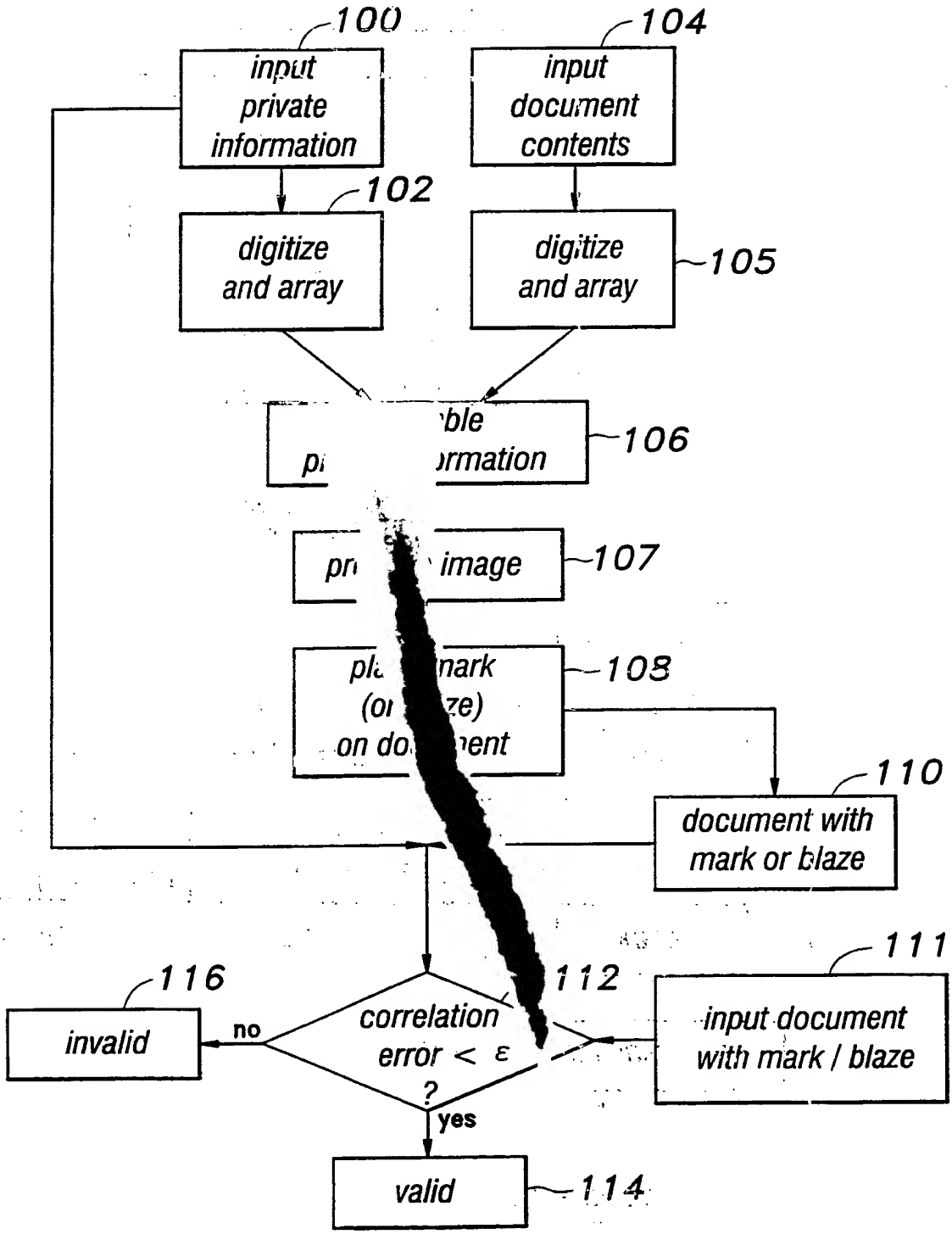


Fig. 12

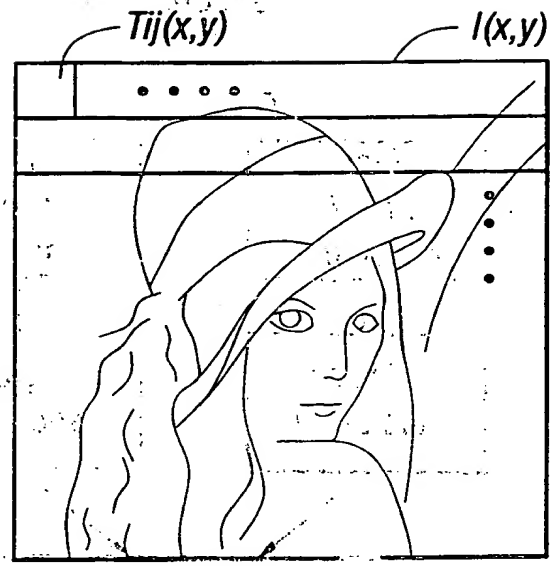
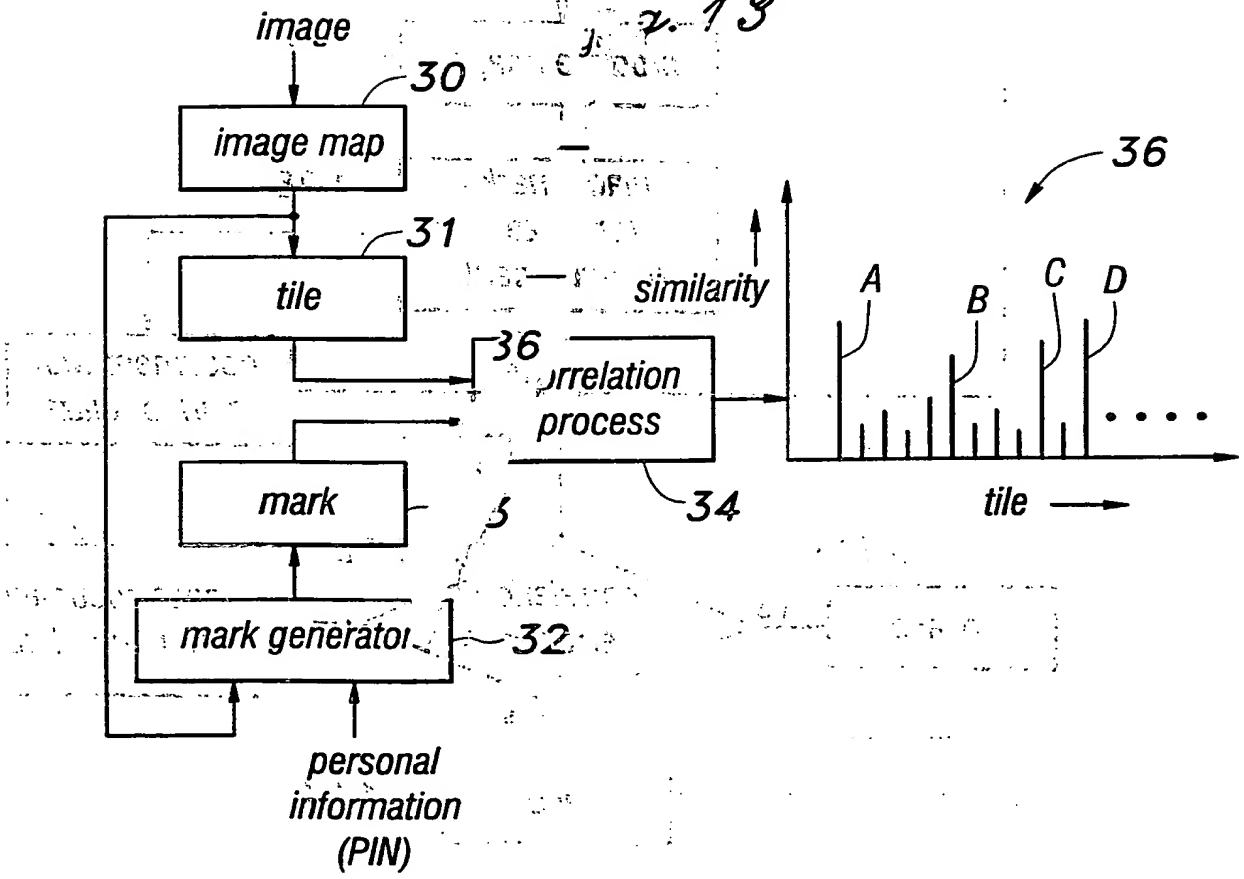


Fig. 13



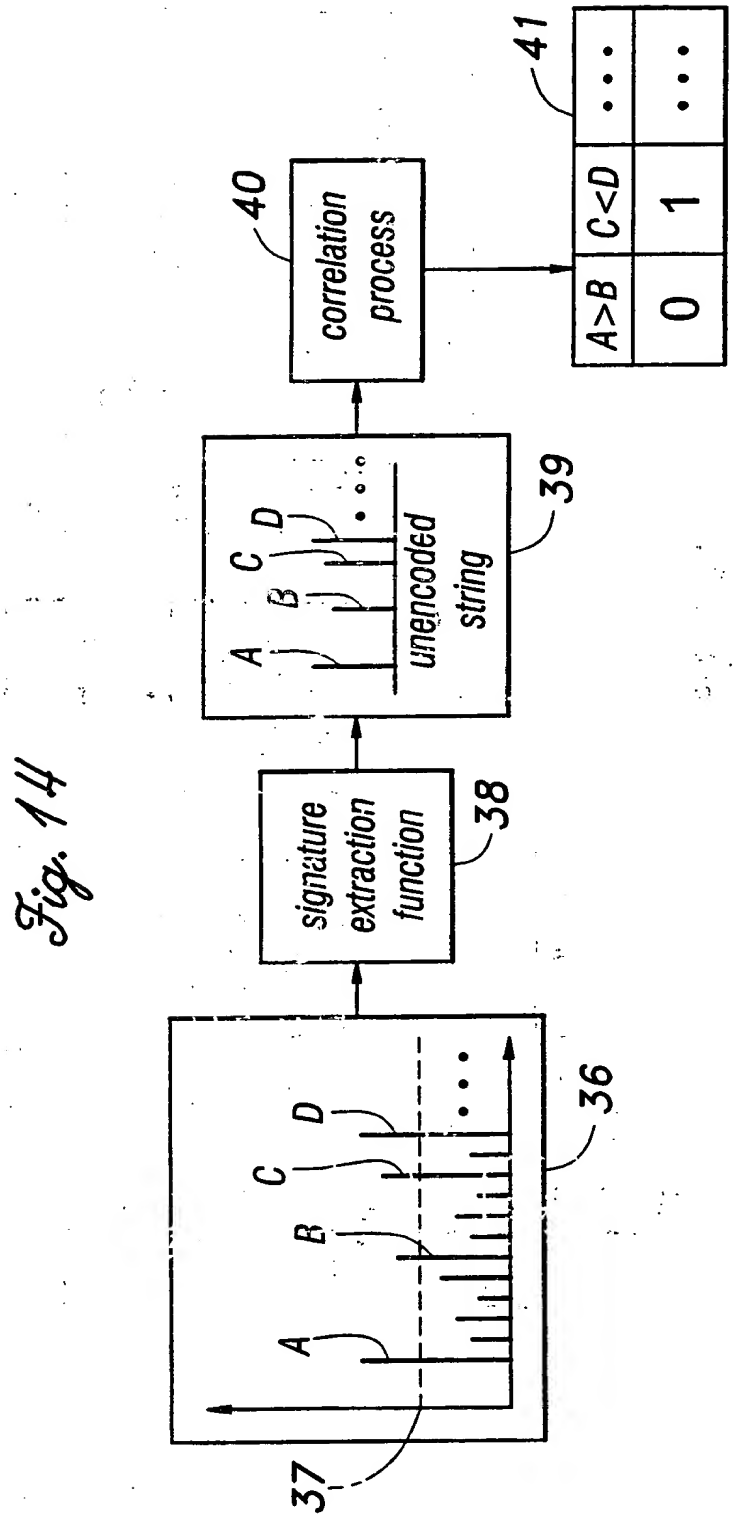


Fig. 14

Fig. 15

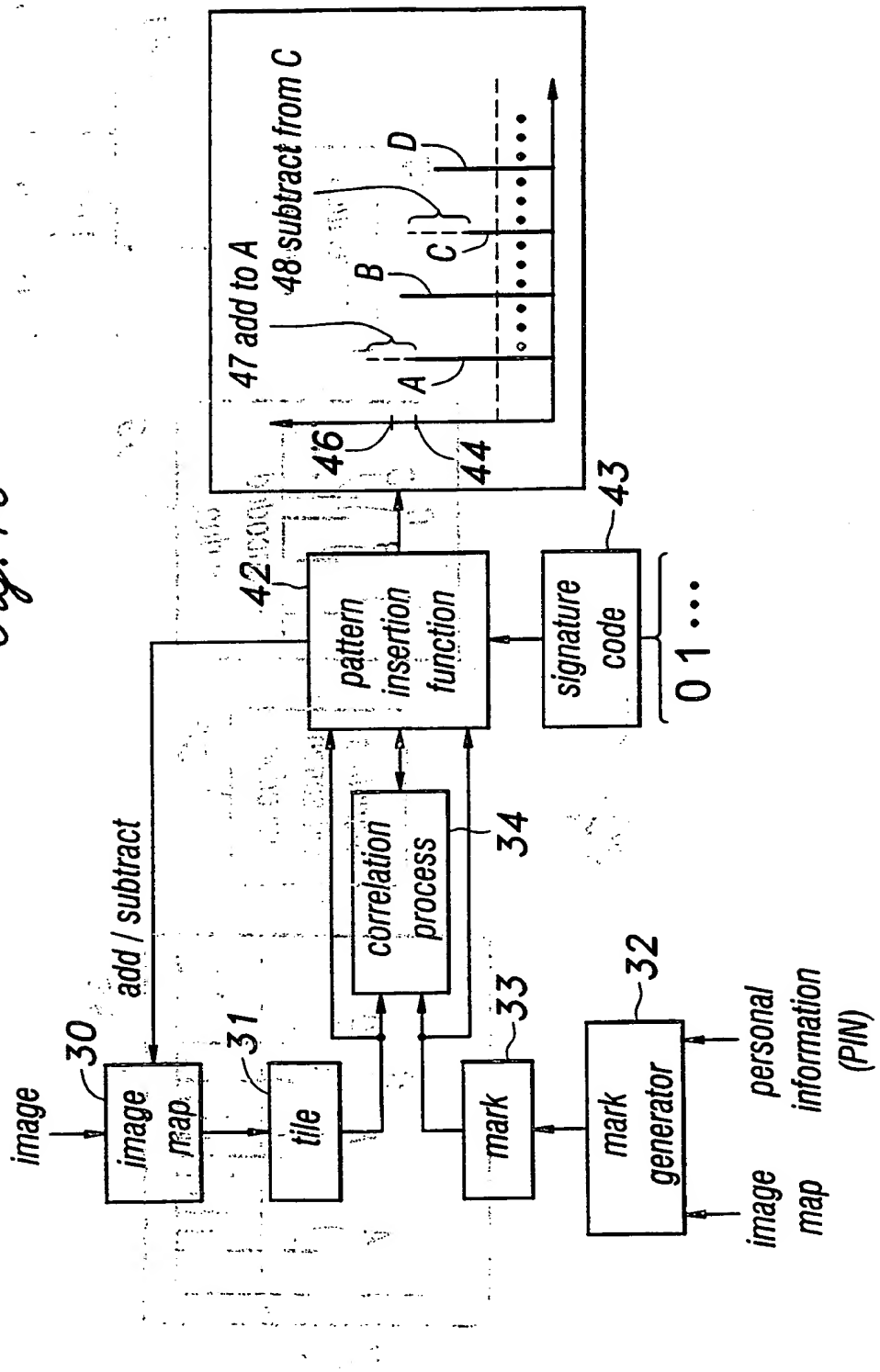
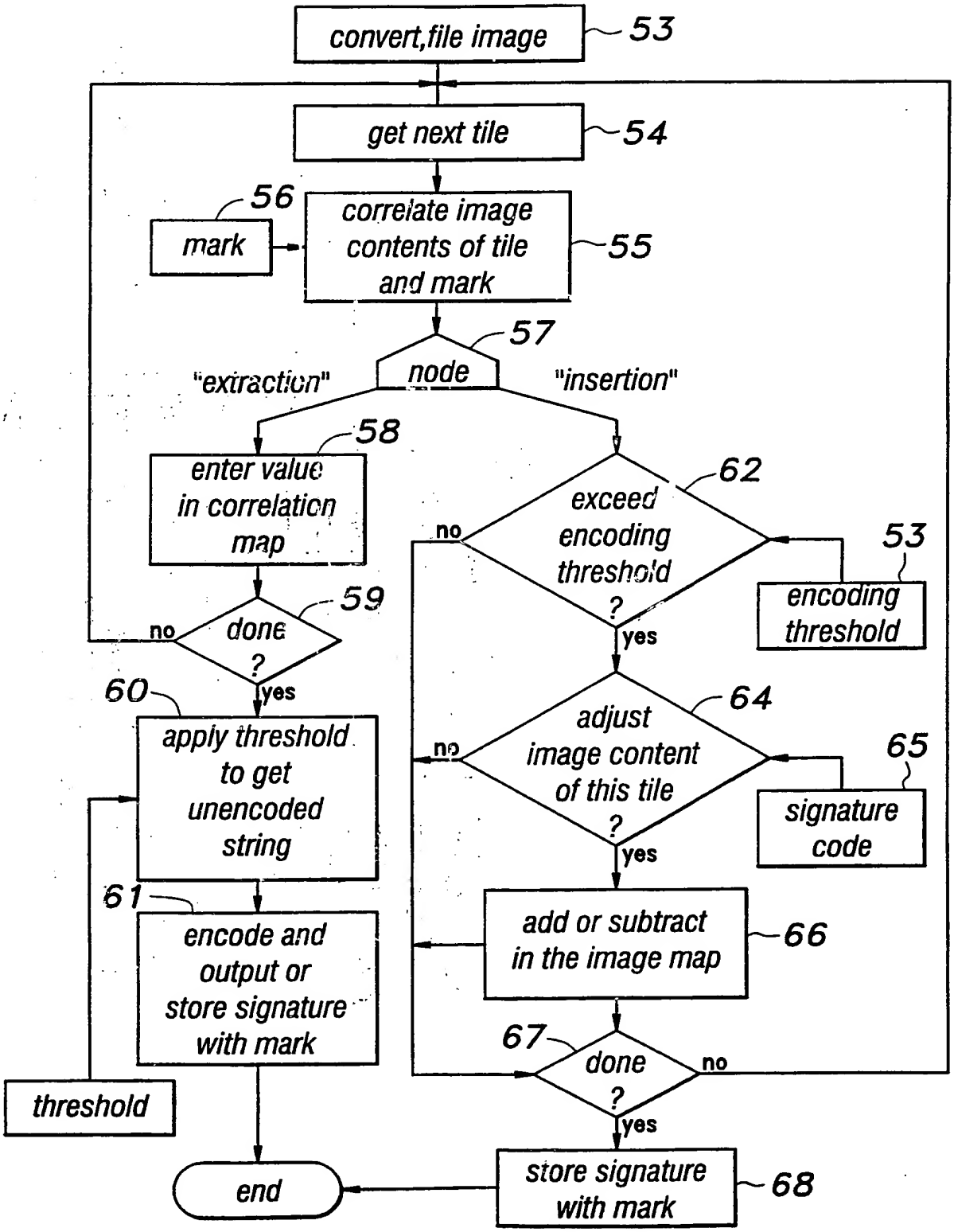


image
30
image map
31
tile
add / subtract
correlation process
34
pattern insertion function
42
47 add to A
48 subtract from C
A
B
C
D
46
44
43
signature code
01...
33
mark
32
mark generator
personal information (PIN)
image map

Fig. 16



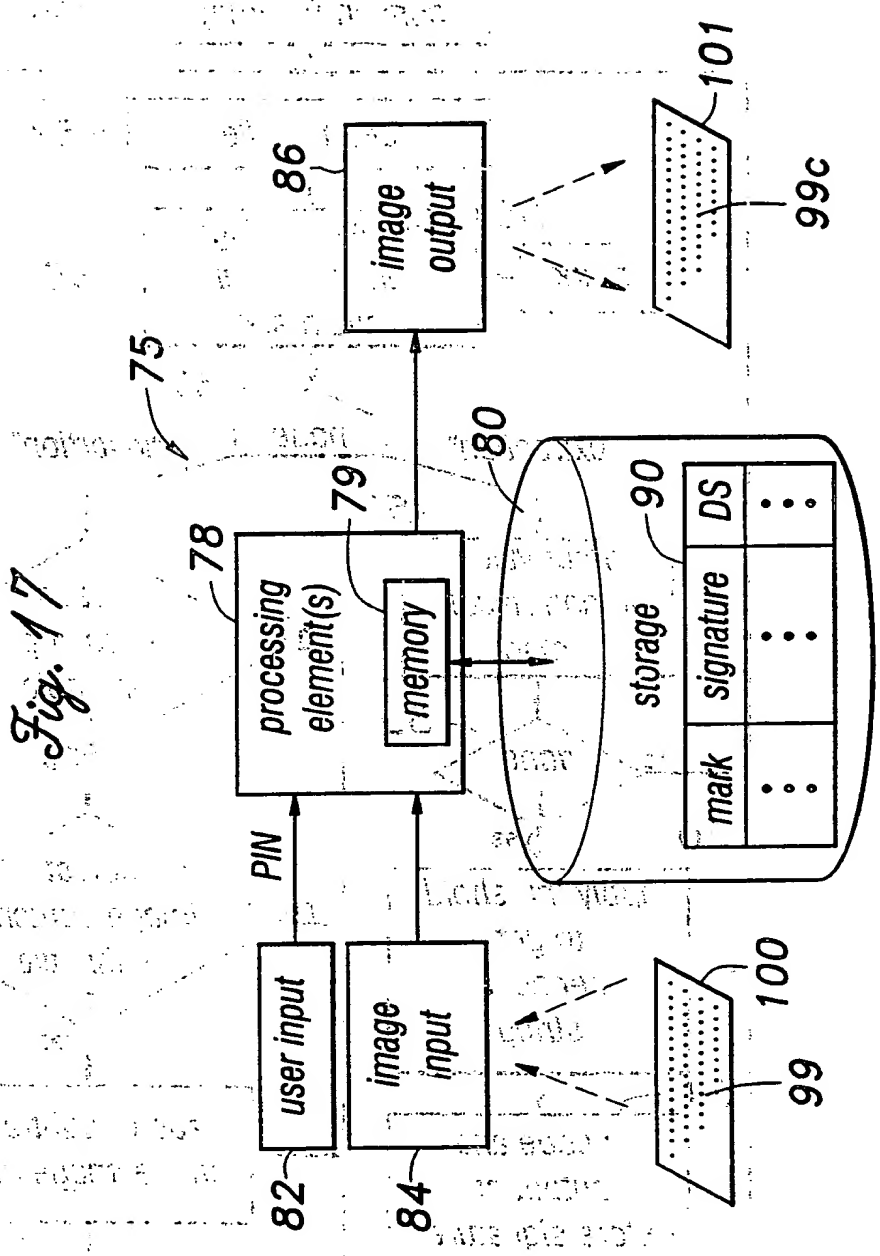


Fig. 17

Fig. 18

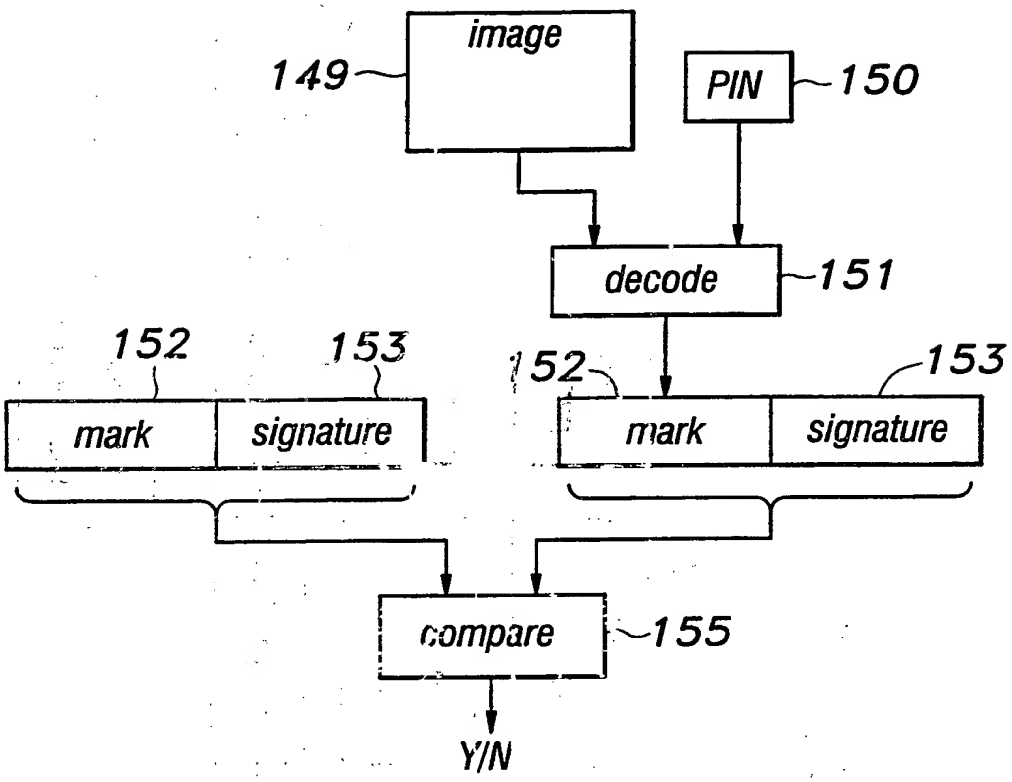
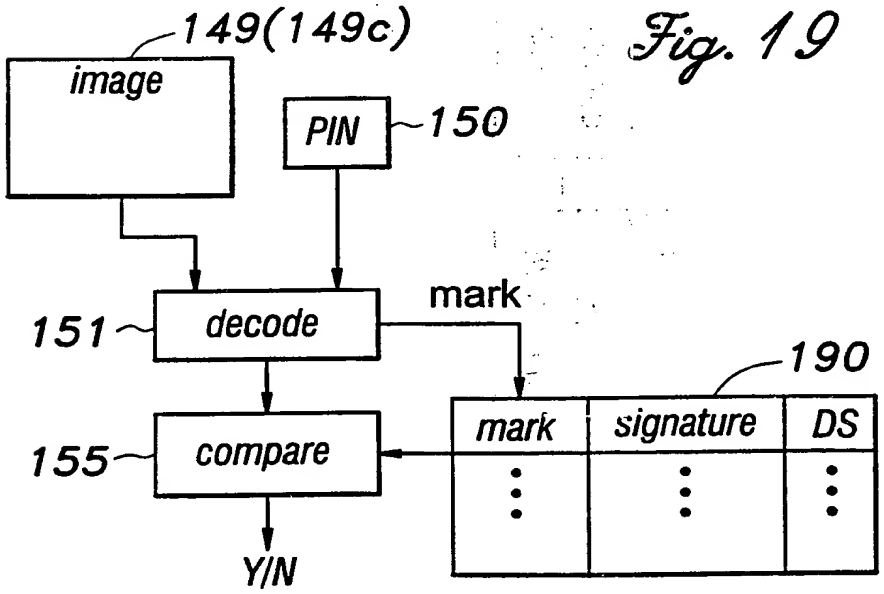


Fig. 19



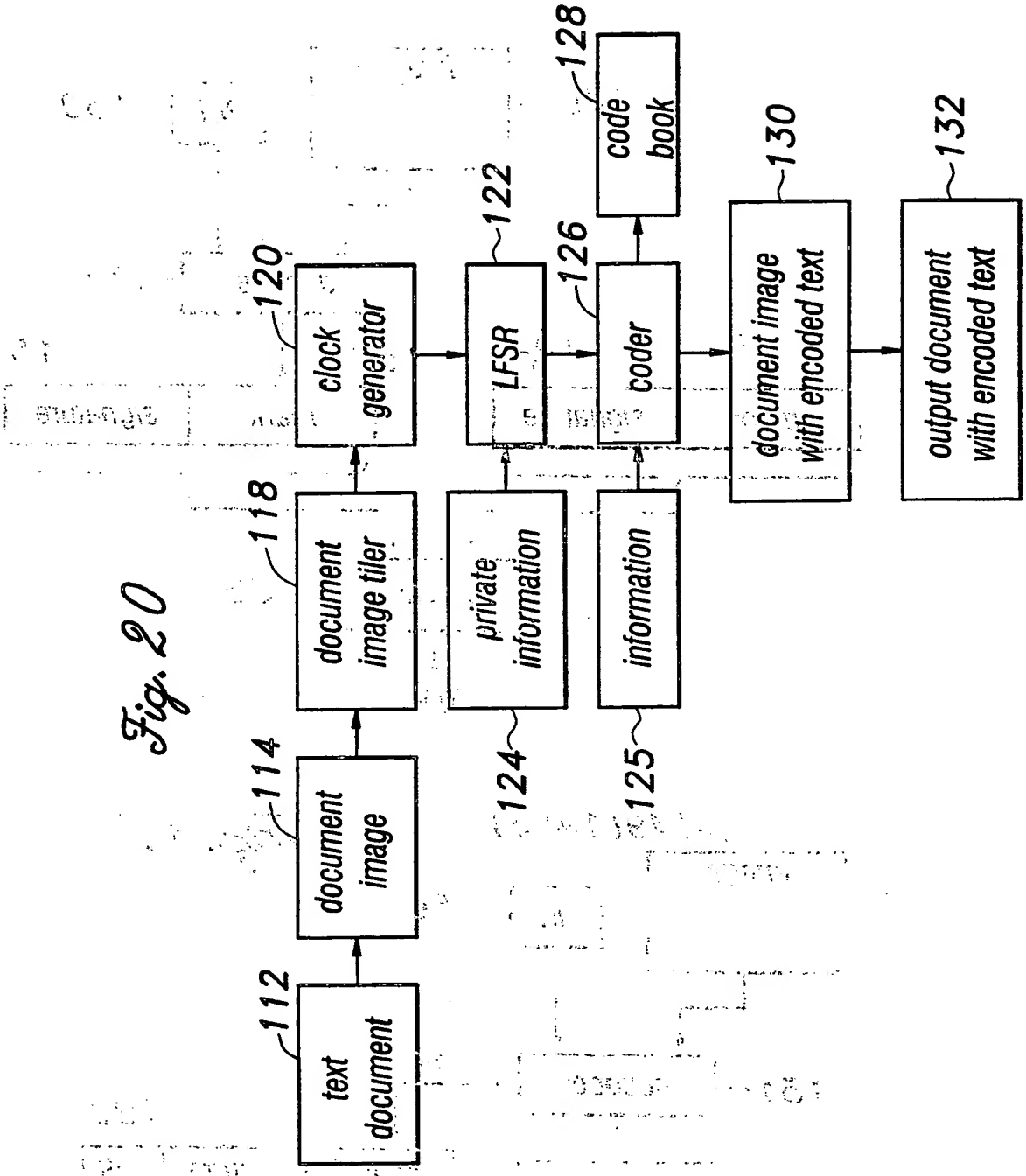


Fig. 20

Fig. 21

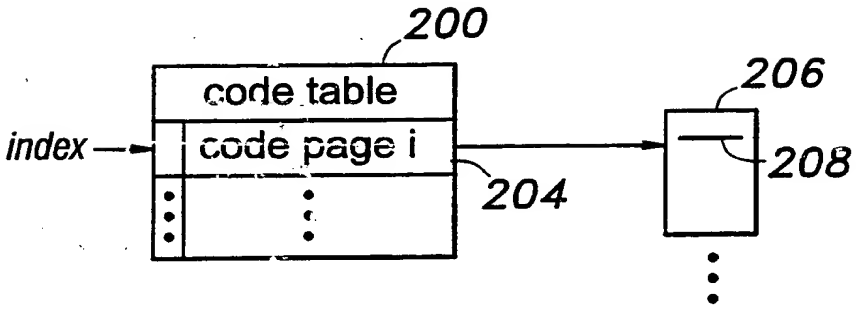


Fig. 22

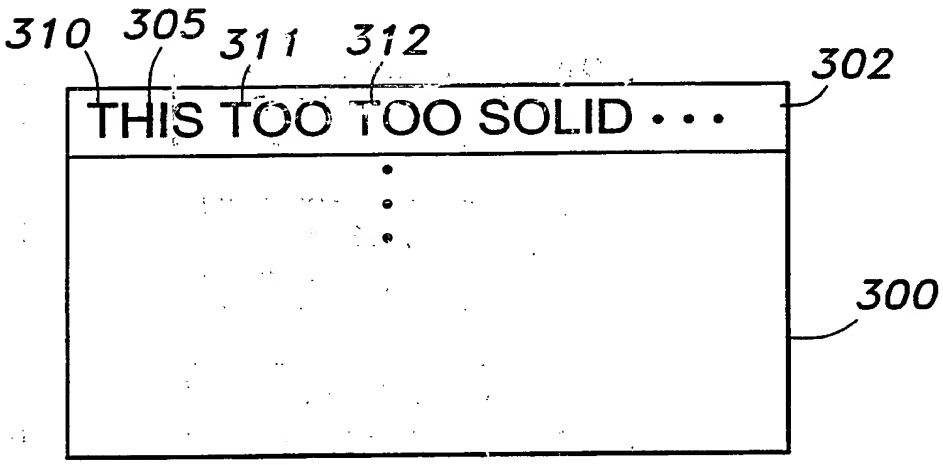


Fig. 23

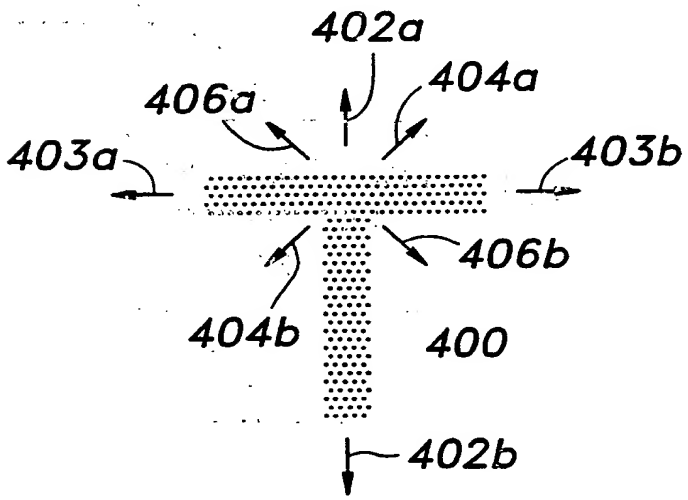
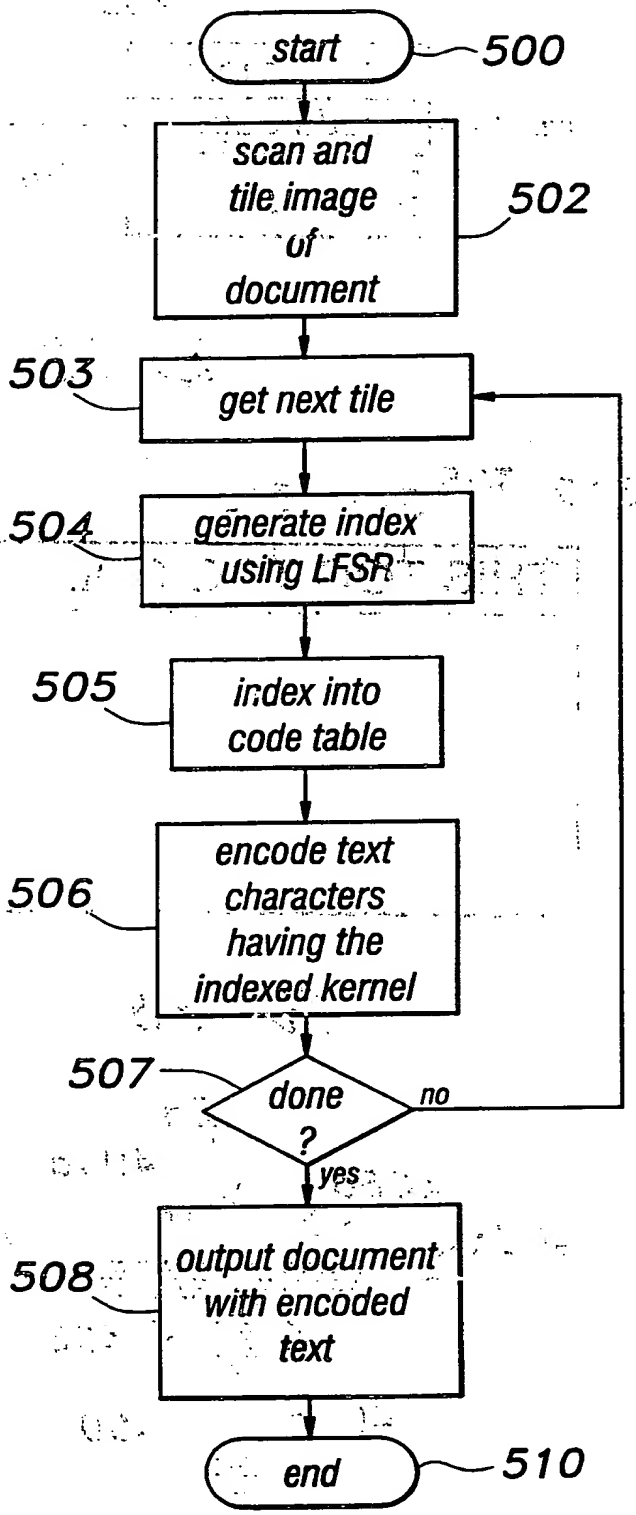


Fig. 24



INTERNATIONAL SEARCH REPORT

Inter. nal Application No
PCT/JP 99/05629

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 27259 A (HIGHWATER FBI LIMITED ;HILTON DAVID (GB)) 6 September 1996 (1996-09-06) the whole document	1-44
A	US 5 613 004 A (MOSKOWITZ SCOTT A ET AL) 18 March 1997 (1997-03-18) abstract column 3, line 48 -column 4, line 67	1-44
A	WO 97 39410 A (HANDEL THEODORE G ;SANDFORD MAXWELL T II (US); UNIV CALIFORNIA (US)) 23 October 1997 (1997-10-23) the whole document	1-44

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 January 2000	27/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Hubeau, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/JP 99/05629

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9627259 A	06-09-1996	AU 4885296 A	18-09-1996
		EP 0813788 A	29-12-1997
		JP 11501173 T	26-01-1999
US 5613004 A	18-03-1997	EP 0872073 A	21-10-1998
		WO 9642151 A	27-12-1996
		US 5687236 A	11-11-1997
WO 9739410 A	23-10-1997	AU 2435297 A	07-11-1997
		US 5819289 A	06-10-1998